Beneficial and Efficient Secure Network Function Virtualization in 5G Wireless Networks

Alwi M Bamhdi

ambamhdi@uqu.edu.sa

Umm Al-Qura University, College of Computing, Al-Qunfudah, KSA

Summary

Future ubiquitous and pervasive networking, wireless apps, and user experiences will be revolutionized by 5G wireless technologies. 5G must deliver vastly increased network capacity to reach its full potential, enabling huge device connections with lower latency and achieving significant energy savings in comparison to current wireless technologies. However, the allocation of virtual resources and duplication of internetworking cache strategies used in 5G are the main challenges in wireless network virtualization. This study proposes an architecture based on information-centric networking and virtual wireless networks to solve the challenges of achieving high resource utilization in 5G networks. The main objective is to use the full potential of 5G in resource leveraging beneficially within the confines of secure network function virtualization. The performance analysis shows that comparing the present non-virtualized architecture to the Virtual Network Functions (VNF), there is a savings of around 30% resources and an amount of money saved by as much as 50%.

Keywords:

5G, network function virtualization, information-centric networking, wireless networks, security.

1. Introduction

The rise of wireless technology as one of the most important developments in networking technology over the previous decade has been well documented. Recent Figures suggest that wireless mobile communication penetration has surpassed that of fixed landline broadband networks, demonstrating that this trend is rising. Recently developed advanced wireless technology and node processing capabilities have made it feasible to build communication networks in addition to providing public broadband access to the internet [1]. This is due to the fact that it is being utilized to offer support for a broad array of innovative multimedia applications and appealing wireless services, which remain fast and gradually grow into a priority at an alarming rate. By 2025, worldwide mobile traffic is expected to have increased by 607 exabytes [2]. To deal with the predicted exponential rise of rich multimedia applications, it is necessary to upgrade cellular networks accordingly to keep up with this expectation. Another challenge with existing wireless communication technology is the utilization of network resources efficiently [3]. To address these challenges, 5G, the fifth generation of wireless telecommunications technology has been introduced. It is positioned to deliver a near-instantaneous response to user input and output delivery with what is commonly known as very low latency. This implies that 5G networks capable of supporting critical applications such as remote surgery and driverless vehicles [4]. The network is also much more responsive than current 4G networks, meaning it can support many more devices at once without slowing down regardless of network load. For example, with 4G we might have a few dozen devices connected at any one time, but with 5G, we can have hundreds of thousands or even millions of devices connected simultaneously. This all sounds great in theory, but there are still some onerous challenges that need to be overcome before starting to use 5G networks on a large scale [5].

The fundamental principles of Network Function Virtualization (NFV) began to emerge in 2010 after the platform as a service (PaaS) model provided by Amazon AWS and other competing vendors caught the majority of the prevalent thinking among practitioners [6]. The early NFV standardization efforts by the European Telecommunications Standards Institute (ETSI) demonstrate this substantial effect on the way hardware virtualization has been crystallized as an essential principle at the foundation of the NFV architectural design [7]. The NFV technology allows wireless network equipment to be separated from its support services. It is possible to create unique services that can use the same infrastructure, allowing them to be used to their full potential. Thus, NFV provides the impetus for new emerging design principles. One such approach is towards software-defined 5G wireless networks, which is an architecture extension of Software Defined Networks (SDN) with the network functions programmable capabilities as required for 5G wireless networks [8]. NFV may virtualize and deploy network operations like as firewalls, intrusion detection and prevention systems, and load balancers as a service on

Manuscript received November 5, 2022
Manuscript revised November 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.11.93

a cloud computing infrastructure. The visualization as Virtual Network Functions (VNFs) are vendor-created software components used to implement network functions creatively and rapidly. NFV leverages the elasticity, on-demand provisioning, and cost-efficiency of the cloud to deliver network functions as a service in the context of network function virtualization [9]. Furthermore, by isolating a portion of the network, Wireless Network Virtualization (WNV) makes it simpler to transit and migrate to newer technologies while still maintaining existing systems as a legacy. The inclusion of NFV in 5G protocols and standards will represent a significant step forward in telecommunications and networking industries. Due to this strategy, a substantial number of data center operators have emerged, who are the owners of commoditized computing platforms and who are prepared to compete openly for the operational needs of network providers that operate a virtualized telecommunication infrastructure [10]. On the one hand, this approach has also produced a number of network operators, who have commoditized their network infrastructure, and are willing to offer their services to the data center operators like utility operators at optimum cost and pricing. On the other hand, the data centre operators are willing to pay a premium for the services provided by the network operators which meet their service level delivery requirements. It is against this background that this paper offers and integrates the WNV and Information-Centric Networking (ICN) to introduce the Information-Centric Wireless Network Virtualization architecture to optimize both service delivery and cost.

2. Network Function Virtualization

The current wireless cellular networks are developed centred on standardized and inflexible hardware components and network architecture. Such designs delay the development of newly emerging wireless technologies, services, and implementation in 5G [11]. One of the most significant and interesting technologies capable of having a dramatic effect on the future 5G wireless networks and the way we refractor the architecture of existing networks is the virtualization of as numerous network functions and resources as possible called NFV. In accordance with the radical paradigm shift in accommodating hardware resources and a stream of services, NFV is anticipated to perform a highly relevant role in 5G wireless networks [12]. NFV intends to virtualize a collection of network functions by initiating them into discrete software packages. These packages can be assembled and connected to a relationship with one another to make the similar services offering a legacy network. The idea of NFV is driven by the traditional server virtualization that can be built by connecting multiple Virtual Machines (VMs) which operate diverse operating systems, software systems, and processes.

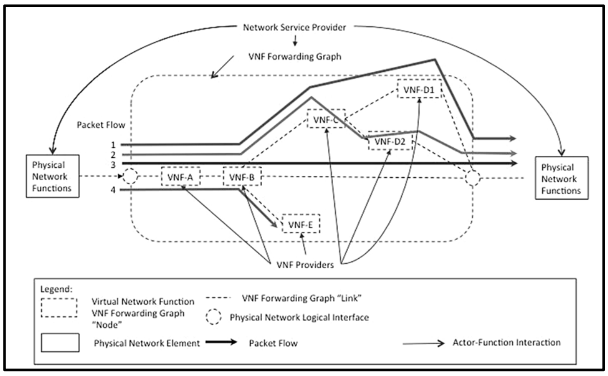

Fig 1. Virtual Network Function Forwarding Graph

In the context of NFV, services are often characterized as a forwarding graph of linked network functions. The forwarding graph distinguishes it, a series of network functions responsible for processing distinct end-to-end flows in the network. One of the most basic illustrations of a forwarding graph may be seen in Fig 1 [13]. In this diagram, the flow of data traverses network functions from the Evolved Node B to the service gateway and then to the Internet Protocol (IP) backbone until it reaches the application server, which is shown as a node in the forwarding graph. In order to meet the needs of mobility management, authentication, and policy enforcement, Non-Access Stratum (NAS) protocols are being moved via diverse network functions. In contrast to existing cellular network technology, which allows a certain function to be engaged on a network-wide scale, forwarding graphs allow 5G operators to supply and activate features for each individual service they provide. The virtualization of network functions is accomplished via the use of a distinct virtualization layer. As a result, this layer decouples service design from service implementation while simultaneously boosting the service's efficiency, robustness, performance, and flexibility [8, 14]. Fig 2 [15], depicts the Network Functions Virtualization (NFV) reference architecture, which can be described as a few forwarding graphs that orchestrate the implementation and operation of Virtual Network Functions (VNFs) across a variety of computing, storage, and networking resources to support a wide range of services. All visible computing and storage resources are typically coupled and shared with one another via the use of networking resources. On the other hand, other network resources link external networks and non-virtualized functions to the VNFs that are already in place, allowing the integration of any technology capable of supporting virtualized 5G network operations to be implemented [16]. The NFV Management and Orchestration system includes resource provisioning components responsible for realizing the potential and reaping the advantages of virtualization.

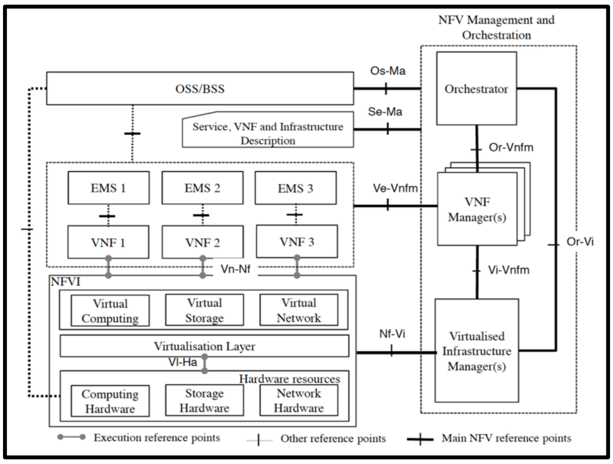

Fig 2. The Network Function Virtualization Architecture

In Fig 2, there are several VNF Managers, each of which performs two key functions: resource provisioning and operations management. The operation of VNF is the responsibility of VNF Managers, and it includes infrastructure management, performance management, fault management, optimization, and capacity planning. While resource provisioning safeguards appropriate resource allocation (for example, allocating VMs to servers), optimal connection across various VNFs, energy conservation, and resource reclamation, resource management ensures optimal resource use. The vast majority of the time, computing, networking, and storage resources are found inside the infrastructure by accident or by design. In 5G Radio Access Networks (RANs) or wireless networks, a reliable and efficient architectural design of VNF Manager may maximize the peak advantages and harness the potential of network functions virtualization (NFV) in order to reduce Capital Expenditures (CAPEX) and Operating Expenditures (OPEX) [17]. This includes dynamic resource allocations, network traffic load balancing, operation and maintenance, and network administration and management. When infrastructure is shared in this way, it can take advantage of the economies of scale projected when it supports numerous logical mobile networks. There are heterogeneous hardware resources, which might be general-purpose, customized, or specialized hardware resources, as well as special-purpose hardware and critical software for hosting mobile network services in the infrastructure. The infrastructure is supplied by a number of infrastructure providers, some of whom are third-party suppliers [18]. The infrastructure providers are responsible for the provisioning of the infrastructure, including the provision of the hardware and software resources, and for the management of the network.

3. Network Problems Raised With NFV

The use of NFV in 5G wireless networks is confronted with a lot of obstacles in terms of networking issues. The NFV technology itself causes these issues, and a number of them are exacerbated by the use of multi-tenant data center networking. When developing NFV platforms for carrier-grade availability, it is necessary to have failover times between redundant 5G VNFs of less than a second, and wireless base stations are actually the ones with the most severe real-time and high-performance constraints, slowing down the development of networks that are reliable and fast [8]. Since the majority of cellular services are behaviorally dynamic, physical resources must be able to grow and contract in response to variations in demand or elasticity. Based on the anticipation that the future 5G network will be very heterogeneous, capacity is directly proportional to the number of nodes, provided that the network follows the rules of centralized interference coordination [9]. Wireless cellular traffic follows predictable patterns that may be seen at any time. If there are any unique occurrences that cause them to alter spatially, it is necessary to allocate resources in the most efficient manner in order to cope with the changes that have happened. Mobility of Virtual Machines (VMs) is a technology capable of enabling quick traffic fluctuations; yet, it comes with its own set of networking design issues.

First and foremost, the migration of a virtual machine to another server must preserve the VM's network information, including the VM's physical location, IP address, and MAC address. Second, the VM implements and supports 5G radio functionalities. It has access to device data, radio channel information, and state channel information, making it critical for VM migration solutions to offer real-time alternatives to distributed state management via cache localization and acceleration agents in order to be successful in the long run. Third, if we are to examine the situation in terms of operational efficiency, it is essential to optimize resource utilization to the greatest extent feasible in order to ensure profitability. It is possible for an operator to recognize and mobilize virtual networks of VNFs on any hardware present in the architecture through the use of an optimal and functional NFV design. This design incorporates resource allocation that is efficient, reliable, effective, and flexible, as well as optimal traffic forwarding through the use of an optimal and functional NFV design architecture [19, 20].

Overhead has a considerable influence on the flexibility and performance of network function virtualization [21]. When experimenting with this phenomenon by deploying many VNFs on the similar physical server, the server will be assigned various addresses rather than a single unique address. The switching networks, in turn, will learn the addresses of each virtual machine, and it can be noted that the size of forwarding tables is increasing at an unmanageable rate. Many service providers share infrastructure at any time. The separation of various VNFs addresses becomes a must in order to avoid conflicts. Separation of VNFs addresses has become necessary. In the case of shared infrastructure, it is important to ensure that the VNFs do not interfere with each other. This is achieved by separating the VNF addresses in the shared infrastructure [22].

Advantage of having multiple service providers share network traffic is that the security, flexibility, and ideal forwarding of traffic from one virtual network to another. Which are not compromised by the fact that the traffic is shared between more than one service provider and that the service providers share networking resources [23, 24].

In order to fully use the promised advantages and actual potential of NFV, it should be possible to preserve the scalability features of already in-use, highly dispersed cellular networks while also using the promised benefits and true potential of NFV. Added functionality, such as load balancing and virtual machine placement, should be real-time aware and enable a wide variety of virtual cellular operations, particularly when used in the cloud context. Figure 3, shows the NFV Architecture in a cloud computing environment [25].

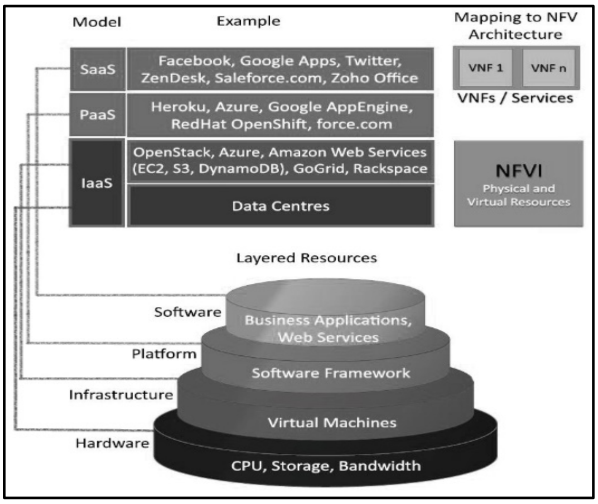

Fig 3. Network Function Virtualization Architecture mapped to Cloud computing service models requirements

4. Wireless Network Virtualization

While using WNV, network infrastructure may be detached from its services, allowing for differentiated services to coexist on the same network infrastructure without conflict. Various service providers (SPs) who run multiple WNV might share the physical wireless networks operated by Mobile Network Operators (MNOs). In general, the logical roles in WNV are those of the SP and the MNO [26]. MNOs are the primary actors in the operation of physical substrate wireless networks, including all infrastructure and radio resources, including as licenced spectrum, radio access networks (RANs), backhaul transmission networks, and core support the networks. The SP is responsible for leasing virtual resources and operating and programming them in order to provide end-to-end services to end customers. Its primary focus is on offering services to subscribers via the use of virtual resources made by MVNO which do not have access to spectrum or radio access networks [27].

5. Information-Centric Networking

ICN is a way to evolve the Internet infrastructure that uses the unique named data technology to enable the transmission of data, which has become necessary due to the increase in the amount of data flow on the internet [28]. Data becomes independent of its location, application, storage, and transit, allowing caching and replication within a network environment. Identifier to location mapping is performed by ICN, and then the route is determined by the pathfinder. A naming strategy in ICN may be classified as either hierarchical, flat, or attribute-based [29]. Hierarchical naming is the most common kind. Every piece of material in the network should be identified by a unique name, which makes it easier for the content provider to transfer the content to the subscriber's device. When compared to the looking for location methodology, this method is more successful. The usage of a distinct name for the material makes it much simpler to determine which route to take in order to access the information.

In ICN, there is also cache-aware routing, for which certain switches are supplied to retain the contents of the cache listed in the routing table. In order to optimize the speed of accessing and delivering the most interesting packet along the way to subscribers as quickly as feasible, a caching method is used. Improved efficiency, increased scalability in response to increased information/bandwidth demand, and improved resilience in demanding communication circumstances are all possible with ICN technology [30, 31]. Furthermore, ICN may be extended to other levels of the protocol stack: named-based data access can be established on top of the current IP infrastructure.

6. Proposed Solution

Virtualization enables the logical separation of software and hardware, whereby the use of the method can reduce the complexity of processing the hardware capacity [32]. Although NFV faces some problems related to transfer data through networking processes, the correct nodes and links have to be correctly selected to optimize the use of physical network components in virtual resource allocation. To achieve a desirably smooth network performance, the WNV has to be integrated with ICN to improve the end-to-end network. To optimize NFV in 5G, an architecture coupling both ICN and WNV is proposed.

It is important to implement network functions over virtualized infrastructures as the NFV undergoes transformation over time to time. The NFV can provide a solution regarding the scalability issues because it only requires the cooperation of many cells, which is usually placed near the network core [33]. There are a few characteristics to overcome NFV problems: one of the characteristics is to decouple VNF addresses from the original physical address through multiple virtual networks. The low amount of Network Virtualization Edges (NVEs) is important where the implementation of the NVEs provides flexibility to deal with high dynamic traffic [34]. Furthermore, the use of Radio Spectrum Resource is important to help in full virtualization whereby multiple operators can share the available radio spectrum. A radio spectrum can have a long-range spectrum that can act as licensed spectrum and be used by unlicensed users [35].

Nevertheless, the use of SDN is another approach to simplify the implementation of network overlay performance. SDN works by the programs it modifies the headers of data packets from different flows and then directly send them to global virtual network addresses [36]. To create virtual resources, a smaller of virtual entities are created from the original physical resources. Basically, a single physical resource includes several elements in the architecture. SDN consists of logical control of a centralised data plane and network management within different controllers. The separation of the two main ideas in SDN gives a chance to switch to not performing control functions in the virtualization of networks. There are two important elements in virtualization infrastructure: efficient virtual resource allocation and the in-network caching strategy are important to map a few processes between virtual and physical resources [37]. Moreover, the efficient use of VNFs enables the network performance to improve because the developers can now have access to the accurate status of the network, maps, parameters, and operator preferences. In the traditional method, content delivery used physical resources from specific operators. With network virtualization into the ICN, the new technologies designed can be implemented faster without troubling the ancient traditional networks [38]. Since the virtualization method and the Information-Centric have been combined together, the content and the physical resources can now be shared with others. To check the overall network performance based on the schemes, a simulation that involves caching capability is run where the location of the macro is placed in the fixed positions in the centre, and the position of other macros is uniformly distributed among themselves.

7. NFV Design Considerations

The evolution of the NFV is not the only thing that needs concentration to make the network connection more efficient and secure [39]. The developers have to take note of a few key considerations as most network users are not concerned with the complexity of the NFV infrastructure.

7.1 Performance

The performance and network infrastructure are the first two critical concerns that must be addressed in order for NFV to be a viable solution for Tunnel Setup Protocols (TSPs). In order to create a dependable solution that meets all of the 5G standards, a significant shift in the network paradigm will be required. In such a revolution, one of the most important issues to consider is the manner in which new network functions are exercised and applied to the value chain. Occasionally, a procedure of this kind necessitates the widespread deployment of specialized devices with 'hard-wired' features and services to achieve the desired results. A significant investment in hardware capabilities is required for any adaptation or upgrade to meet the ever-increasing and diverse market demands [40]. NFV designs must be improved in order to attain the desired network performance that may be obtained from the running programs in the hardware. This will require upgrading every element in the architecture, which is vital for the network. They must make full use of all available interfaces and methods, such as direct memory access (DMA) for the transfer of connection data, in order to achieve success [41]. The usage of Data Plane Development Kits (DODKs) and Field-Programmable Gate Arrays (FPGAs) has been shown to be an appropriate method of improving VNFs [42]. A storage infrastructure with computational resources should be used for the implementation of VNFs; otherwise, the NFV would demand additional resources.

7.2 Security

Security and resilience are also important because, lately, the nature of the NFV relies on security technologies and policies [43]. In fact, the design of the NFV has two important security measures that have to be considered. Firstly, the functions or services must be protected from different users. These security measures help to make sure that there is no failure in the security system or maybe a network security breach, but if that case happens, the failure service/function will not affect others in the system. There are a few ways to secure the NFV designs. One of the ways is to deploy firewalls within the virtual environment to allow access to VNFs without allowing malware from entering the networks [44].

7.3 Relatability and Availability

Reliability and availability play an important role in key considerations where the telecommunications and the service recovery of the NFV are performed automatically [45]. Nowadays, network users expect high reliability and availability in their network connections as TSPs are often considered an important part of the infrastructure. The framework of the NFV must support the availability requirements to avoid software and hardware crashes [46]. Moreover, the heterogeneity support for NFV is an acceptable key solution where the main objective of introducing the NFV is to break the barriers from hardware provision. The NFV platform must include all the required elements, whereby the platform must be capable of sharing the environment with different developers. The platform must be flexible to use by many running applications. The platforms also must support the end-to-end services without blockage for more specific technology solutions. NFV allows for continuous growth to enhance the productivity of internal functions and results. In every new technology introduced, the system's compatibility is very important to make the system run smoothly. This role is called legacy support, whereby it is important for any telecommunication company to apply this type of design to have user trust. This is a strategy to close the gap between the NFV and the supporting services.

As acknowledged by leading experts, NFV has some meaningful benefits in improving network connection performance. It is necessary to have a responsive and scalable network solution to achieve that. The NFV must be able to support a huge number of users. All of the functions in the machines must be able to function flawlessly, or else they cannot meet the user requirement and expectations of a given function.

8. WNV and ICN

Physical radio resources and cellular network infrastructure resources may be diverted and separated into virtual cellular network resources that have certain identical features and can be shared by numerous parties by physically isolating them. As the author of [47] put it, virtualizing mobile cellular networks is the act of splitting, separating, and sharing mobile cellular networks in order to make them more accessible to more people. The physical resources of cellular networks, in general, consist of infrastructure resources and licensed spectrum resources, which include core networks, radio access networks (RANs), and transport networks (TNs). However, ICN has piqued the attention of both academia and business [48] because the communication paradigm inside ICN is distinct from the IP communication paradigm. Present-day IP networks operate on the basis of a host-based conversation model, with data being transported via the network in accordance with a source-driven paradigm. Aside from that, the author of [8] noted that the primary job of ICN is to distribute, discover, and transmit information rather than to ensure that end hosts are reachable and that talks between them are maintained in the network. It is common in ICN for users to request material without knowing which host is able to deliver it. Communication takes place using a receiver-driven paradigm, and information is sent in a reverse way [49].

In ICN, the network is in charge of creating a mapping between requested content and its location. The match between requested content and its location determines the development of a link between the network and the content location. Information-centric wireless network virtualization (ICWNV) is a new architecture that we propose to enable WNV with ICN support. Dedicated physical resources from a single operator were utilized for content distribution [50]. The network becomes more complicated because physical resources cannot be shared between several operators. In a coincidental way, WNV facilitates the sharing of infrastructure as well as content across various service providers. By incorporating network virtualization into ICN, new networking technologies may be developed and implemented without having an impact on existing networks that are specifically built for ICN use. Furthermore, combining virtualization with ICN makes it possible to share both physical resources and content. Since duplication of content transfers absorb real resources and share material via virtual networks, it is possible to reduce the number of unwanted duplicative transmissions made.

On the other hand, Radio Spectrum Resource is considered as one of the most crucial resources in wireless communication and networking [51]. With spectrum sharing, the licensed spectrum held by the operator may be used to its maximum potential. On the other hand, Spectrum sharing is not popular due to politics and economics rather than because of technological advances. However, spectrum sharing is a crucial component of WNV since it allows all of the numerous operators to share all of the available radio spectrum in order to enable complete virtualization of the network. Furthermore, Wireless Network Infrastructure (WNI) is a critical component of a cellular network's infrastructure. Network sharing may be defined as the situation in which numerous

MNOs share the same physical network infrastructure with one another. Virtual resources are created by splitting physical resources into several virtual slices and combining the results. All of the virtual entities sliced by each element in WNI should ideally be included in a single slice, rather than being spread over many slices. There is no ambiguity about the fact that some MVNOs simply need RAN slices since they have their own centered network but no radio coverage [52]. As a result, various requirements will need varying degrees of virtualization. In terms of wireless virtual resources, there are three basic layers of slicing to consider: content-level slicing, network-level slicing, and flow-level slicing. WNV is the best case for content-level slicing, and network-level slicing is ideal for network-level slicing. Flow-level slicing is often a collection of flows belonging to an entity that needs virtualized resources from MNOs [53].

Taking use of the capabilities of WNV and ICN techniques, we presented an Information-Centric - WNV architecture that strives to enhance the overall network performance from start to finish. It is possible to share both physical resources and content across various SPs when these strategies are used in conjunction. Apart from that, this methodology is capable of reducing duplication of transmission in the network, where it may eliminate any unneeded material in comparison to the previous method of transmission. Physical wireless networks information-Centric-WNV are virtualized into two virtual networks, with one virtual network operating on the Information-Centric Network and the other virtual network running on the conventional network.

Since the WNV technique allows the physical resources and contents to be shared among SPs, this technique also permits to share the radio spectrum among different operators. In wireless networks, the radio spectrum is the most vital resource which is divided into two categories: licensed radio spectrum and free radio spectrum. Thus, it is possible to share the licensed spectrum that is owned by one operator with another operator based on an agreement. Besides sharing the radio spectrum, the physical infrastructure component can also be shared with more than one MNO. These MNOs share the resources that they have to develop a complete network. An MNO may not have an infrastructure component, but the network infrastructure can still be developed using the components owned by the other MNO. So, the MNOs are able to gain benefits from cooperating with each other.

The proposed architecture highlights the important component of efficient virtual resources allocation and in-network caching strategy. Firstly, MVNOs need to select the appropriate infrastructure and radio spectrum from various leased infrastructures. The MVNOs need to make a good decision about which infrastructure components they want to use in order to fulfill the requirements of virtual resources. The selected physical resources will be mapped with the virtual resources by applying some virtualization procedure. The binary control variable may recognize the virtual resources allocation $\boldsymbol{x_{ki}}$. $\boldsymbol{x_{ki}}$ become 1, if the infrastructure $\boldsymbol{i}$ with $\boldsymbol{i} \in \triangleq \{\mathbf{1}, \mathbf{2}, .., \boldsymbol{I}\}$ is selected for mobile user $\boldsymbol{k}$ with $\boldsymbol{k} \in \boldsymbol{K} \triangleq \{\mathbf{1}, \mathbf{2}, .., \boldsymbol{K}\}$; otherwise $\boldsymbol{x_{ki}} = 0$. Then, the formula is given in Eq. 1 [8] used to calculate the average gain achieved by the resource virtualization to determine whether the infrastructure component is suitable with the virtual resources. $\boldsymbol{r_{ki}}$ is gain obtained through the resources virtualization.

$$E\left[Gain_{virtualization}\right] = \sum_{k \in K, i \in I} r_{ki} x_{ki} y_{ki} \tag{1}$$

For caching strategies, we also use the binary control variable method z_{kj} where z_{kj} is 1 if network element j with $j \in J \triangleq \{1,2,..,J\}$ caches the content requested by mobile user k with $k \in K$; otherwise $z_{kj} = 0$. The same goes for caching strategies; we need to calculate the gain achieved by the caching strategies by using the formula below. q_k is request rate of the content and o_{kj} is gain obtained through caching represented in Eq.2 [8].

$$E\left[Gain_{caching}\right] = \sum_{k \in K, j \in J} q_k o_{kj} z_{kj} \tag{2}$$

The aim is to minimize the inter-ISP traffic, intra-ISP traffic (RAN), and content access delay in the network. We will formulate the virtual resource allocation and in-network caching strategies to find the maximum binary in one resource as below where U_v and U_c are two utility functions for $E[Gain_{virtualizationn}]$ and $E[Gain_{caching}]$ respectively shown in Eq. 3 [8].

$$\sum_{k \in K, j \in I} U_v\left(E\ Gain_{virtualization}\right) + \sum_{k \in K, j \in J} U_c\left(E\ Gain_{caching}\right) \tag{3}$$

9. Performance Analysis

9.1 NFV over 5G Wireless Network

Network virtualization may be seen as a technique of sharing the whole network system with an optimal conception. RANs may be made more energy efficient by virtualizing numerous control and user plane network operations. This can be accomplished via dynamic infrastructure resource allocation and traffic balancing, which reduces the footprint and energy usage. Considering the real-world traffic mix of a cellular network, where the network consists of 85 cells and the traffic trails over a period of 6 hours. In their traces, a voice call consumes one processing unit per second, whereas a packet session consumes two processing units per second, and so on. A single dedicated baseband processing unit (BBU) has a capacity ranging from 64 to 256 processing units, depending on whether it is virtualized or not, and it may be virtualized. In proportion to the growth in the maximum capacity of the BBU, the total number of BBU needed falls with VNFs, reaching a maximum of 25 percent when the BBU promotes 256 processing units, as shown in Figure 4

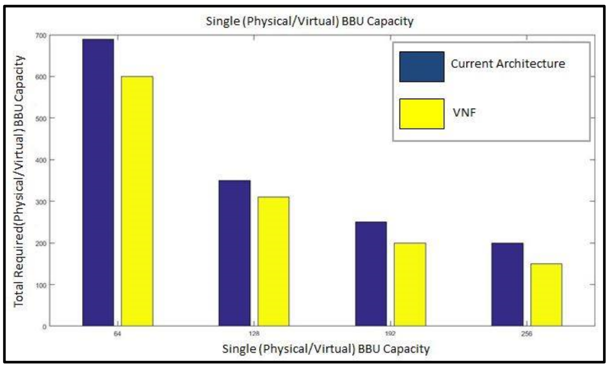

Fig 4. Capacity comparison of BBU with respect to NFV

The average number of active BBUs may be used to calculate the amount of OPEX savings. In the proposed NFV architecture, traffic from any site is routed to one or more virtual BBUs that are currently operational and have sufficient usage before activating another virtual BBU. When comparing the present non-virtualized architecture to the VNF, there is a savings of around 30%. Increasing the maximum BBU capacity to 256 improves the amount of money saved by as much as 50%, given in Figure 5.

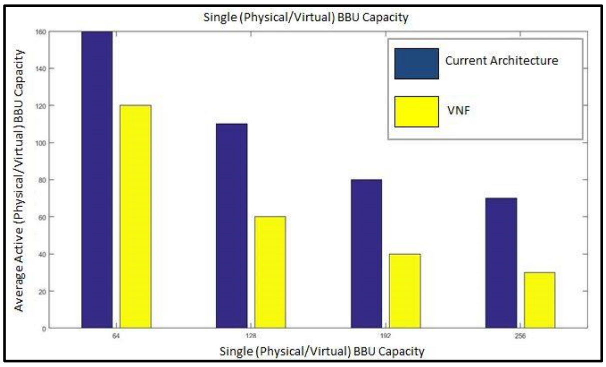

Fig 5: Cost saving comparison of BBU with respect to NFV

9.2 ICN over 5G Wireless Network

An extremely flexible 5G network that can adapt to the dynamism of traffic location and pattern requires the ability to dynamically assign more or fewer units of computational power to the virtual cells that are distributed throughout the network. This is achieved by using a Radio Access Network [20]. A simulation is carried out in order to estimate the performance of the suggested virtual resources allocation and in-network caching strategies. The simulation is based on a heterogeneous network with in-network caching capabilities. Two RAN infrastructure providers (InPs), two backhaul infrastructure providers (InPs), one MVNO, and three service providers (SPs). RAN InP1 is the owner of a two-tier cellular network consisting of one macro base station and six mini base stations. RAN InP2 is in possession of six tiny BSs. The placement of the macro BS is established in the middle, and the distribution of the 12 tiny BSs is consistent. According to the accompanying graph, as shown in Figure 6, the suggested design with in-network caching reduces overall backhaul utilization compared to the old system.

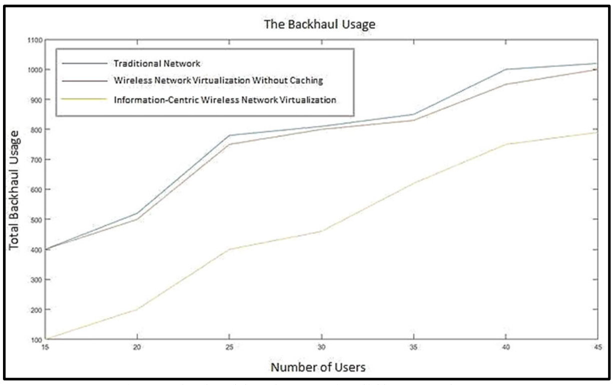

Fig 6. The backhaul usage in different schemes

In this comparison, as shown in Figure 6, the number of consumers who are satisfied with the least data rate requirement demanded by the service providers (SPs) is calculated. The implementation of NFV may be completed without compromising data rate requirements. When compared to the overall number of users in the conventional system, the number of satisfied users is lower in the alternative plan.

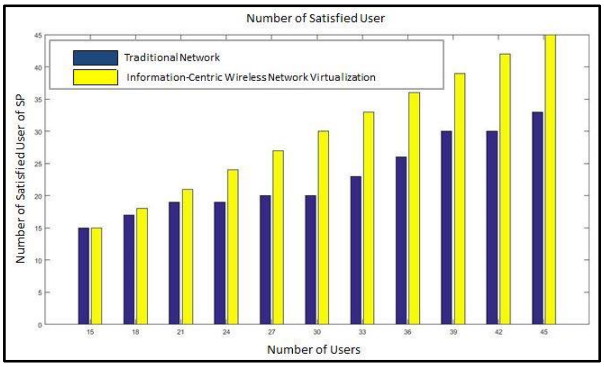

Fig 7. The number of total satisfied user of SPs

10. Conclusion

This paper presented thorough studies, research and challenges on Network Function Virtualization. Different techniques and methods were used to prove that the use of NFV in 5G is suitable for not only for today's needs but also into the future enhancements and innovation because of the visualization and programmable software defined network approaches. Even though virtual resource allocation and duplication of in-network caching strategies used in 5G are the main challenges in WNV, those problems can be easily solved by using the proposed methods in this paper as vouched by the experimental results. These results clearly show that the technique used can increase not only the performance where more devices securely enter the 5G network with less traffic congestion but also offer considerable cost savings to service providers. Despite its fabulous design and well-being, the flexibility and throughput of a 5G network needs further studies and research when it comes to determining its security risk analysis comprehensively as possible for its operational functionality and service levels of behavior [54]. It also requires determining advanced security solutions and intrusion detection [55] and protection mechanisms [56] through future research and subsequent operational deployment and use in 5G networks. This research door is open for anyone embarking in a career on 5G networking accommodating a host of multimedia and management of their combined operations.

Acknowledgments

This work was supported by Umm Al-Qura University through my employment.

References

[1] Akyildiz, I. F., Kak, A., & Nie, S. (2020). 6G and beyond: The future of wireless communications systems. IEEE access, 8, 133995-134030.

[2] Hewa, T., Gür, G., Kalla, A., Ylianttila, M., Bracken, A., & Liyanage, M. (2020, March). The role of blockchain in 6G: Challenges, opportunities and research directions. In 2020 2nd 6G Wireless Summit (6G SUMMIT) (pp. 1-5). IEEE.

[3] Hakiri, A., & Berthou, P. (2015). Leveraging SDN for the 5G networks: trends, prospects and challenges. arXiv preprint arXiv:1506.02876.

[4] Rao, S. K., & Prasad, R. (2018). Impact of 5G technologies on smart city implementation. Wireless Personal Communications, 100(1), 161-176.

[5] Taleb, T., Samdanis, K., Mada, B., Flinck, H., Dutta, S., & Sabella, D. (2017). On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration. IEEE Communications Surveys & Tutorials, 19(3), 1657-1681.

[6] Wang, G., & Ng, T. E. (2010, March). The impact of virtualization on network performance of amazon ec2 data center. In 2010 Proceedings IEEE INFOCOM (pp. 1-9). IEEE.

[7] Chatras, B. (2018). On the standardization of NFV management and orchestration APIs. IEEE Communications Standards Magazine, 2(4), 66-71.

[8] Liang, C., Yu, F. R., & Zhang, X. (2015). Information-centric network function virtualization over 5G mobile wireless networks. IEEE network, 29(3), 68-74.

[9] Abdelwahab, S., Hamdaoui, B., Guizani, M., & Znati, T. (2016). Network function virtualization in 5G. IEEE Communications Magazine, 54(4), 84-91.

[10] Pianese, F., Gallo, M., Conte, A., & Perino, D. (2016, April). Orchestrating 5G virtual network functions as a modular Programmable Data Plane. In NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium (pp. 1305-1308). IEEE.

[11] Le, L. B., Lau, V., Jorswieck, E., Dao, N. D., Haghighat, A., Kim, D. I., & Le-Ngoc, T. (2015). Enabling 5G mobile wireless technologies. EURASIP Journal on Wireless Communications and Networking, 2015(1), 1-14.

[12] Ameigeiras, P., Ramos-Munoz, J. J., Schumacher, L., Prados-Garzon, J., Navarro-Ortiz, J., & Lopez-Soler, J. M. (2015). Link-level access cloud architecture design based on SDN for 5G networks. IEEE network, 29(2), 24-31.

[13] Lee, B., Murray, N., & Qiao, Y. (2015). Active accounting and charging for programmable wireless networks. Mobile Networks and Applications, 20(1), 111-120.

[14] Wen, R., Feng, G., Tan, W., Ni, R., Qin, S., & Wang, G. (2017). Protocol function block mapping of software defined protocol for 5G mobile networks. IEEE Transactions on Mobile Computing, 17(7), 1651-1665.

[15] Alnaim, A., Alwakeel, A., & Fernandez, E. B. (2019, August). A misuse pattern for compromising vms via virtual machine escape in nfv. In Proceedings of the 14th International Conference on Availability, Reliability and Security (pp. 1-6).

[16] Neves, P., Calé, R., Costa, M., Gaspar, G., Alcaraz-Calero, J., Wang, Q., & Preto, R. (2017). Future mode of operations for 5G–The SELFNET approach enabled by SDN/NFV. Computer Standards & Interfaces, 54, 229-246.

[17] Sairam, R., Bhunia, S. S., Thangavelu, V., & Gurusamy, M. (2019). NETRA: Enhancing IoT security using NFV-based edge traffic analysis. IEEE Sensors Journal, 19(12), 4660-4671.

[18] Sayadi, B., Gramaglia, M., Friderikos, V., Hugo, D. V., Arnold, P., Alberi-Morel, M. L., & Crippa, M. R. (2016, May). SDN for 5G Mobile Networks: NORMA perspective. In International Conference on Cognitive Radio Oriented Wireless Networks (pp. 741-753). Springer, Cham.

[19] Kalim, U., Gardner, M. K., Brown, E. J., & Feng, W. C. (2013, July). Seamless migration of virtual machines across networks. In 2013 22nd International Conference on Computer Communication and Networks (ICCCN) (pp. 1-7). IEEE.

[20] Monserrat, J. F., Alepuz, I., Cabrejas, J., Osa, V., López, J., García, R., & Soler, V. (2016). Towards user-centric operation in 5G networks. EURASIP Journal on Wireless Communications and Networking, 2016(1), 1-7.

[21] Wood, T., Ramakrishnan, K. K., Hwang, J., Liu, G., & Zhang, W. (2015). Toward a software-based network: integrating software defined networking and network function virtualization. IEEE Network, 29(3), 36-41.

[22] Ordonez-Lucena, J., Ameigeiras, P., Lopez, D., Ramos-Munoz, J. J., Lorca, J., & Folgueira, J. (2017). Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges. IEEE Communications Magazine, 55(5), 80-87.

[23] Khan, A. S., Javed, Y., Abdullah, J., Nazim, J. M., & Khan, N. (2017). Security issues in 5G device to device communication. IJCSNS, 17(5), 366.

[24] Khan, S., Abdullah, J., Khan, N., Julahi, A. A., & Tarmizi, S. (2017). Quantum-elliptic curve cryptography for multihop communication in 5G networks. International Journal of Computer Science and Network Security (IJCSNS), 17(5), 357-365.

[25] Mijumbi, R., Serrat, J., Gorricho, J. L., Bouten, N., De Turck, F., & Boutaba, R. (2015). Network function virtualization: State-of-the-art and research challenges. IEEE Communications surveys & tutorials, 18(1), 236-262.

[26] Habiba, U., & Hossain, E. (2018). Auction mechanisms for virtualization in 5G cellular networks: basics, trends, and open challenges. IEEE Communications Surveys & Tutorials, 20(3), 2264-2293.

[27] Wang, X., Krishnamurthy, P., & Tipper, D. (2013, January). Wireless network virtualization. In 2013 international conference on computing, networking and communications (ICNC) (pp. 818-822). IEEE.

[28] Amadeo, M., Campolo, C., Quevedo, J., Corujo, D., Molinaro, A., Iera, A., & Vasilakos, A. V. (2016). Information-centric networking for the internet of things: challenges and opportunities. IEEE Network, 30(2), 92-100.

[29] Nour, B., Sharif, K., Li, F., Moungla, H., & Liu, Y. (2020). A unified hybrid information-centric naming scheme for IoT applications. Computer Communications, 150, 103-114.

[30] Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., & Ohlman, B. (2012). A survey of information-centric networking. IEEE Communications Magazine, 50(7), 26-36.

[31] Khan, N. A. (2022). PKI-Based Security Enhancement for IoT in 5G Networks. In Inventive Computation and Information Technologies (pp. 217-225). Springer, Singapore.

[32] Ma, Z., Zhang, Z., Ding, Z., Fan, P., & Li, H. (2015). Key techniques for 5G wireless communications: network architecture, physical layer, and MAC layer perspectives. Science China information sciences, 58(4), 1-20.

[33] Khan, N., & Alzaharani, M. Y. (2018). Establishing EndVisor and Quarantine Approach in Solving Security Issues of Virtualization. Indian Journal of Science and Technology, 11, 47.

[34] Alaluna, M., Vial, E., Neves, N., & Ramos, F. M. (2019). Secure multi-cloud network virtualization. Computer Networks, 161, 45-60.

[35] Moon, B. (2017). Dynamic spectrum access for internet of things service in cognitive radio-enabled LPWANs. Sensors, 17(12), 2818.

[36] Feamster, N., Rexford, J., & Zegura, E. (2014). The road to SDN: an intellectual history of programmable networks. ACM SIGCOMM Computer Communication Review, 44(2), 87-98.

[37] Liang, C., Yu, F. R., Yao, H., & Han, Z. (2016). Virtual resource allocation in information-centric wireless networks with virtualization. IEEE Transactions on Vehicular Technology, 65(12), 9902-9914.

[38] Ghosh, U., Chatterjee, P., Tosh, D., Shetty, S., Xiong, K., & Kamhoua, C. (2017, June). An SDN based framework for guaranteeing security and performance in information-centric cloud networks. In 2017 IEEE 10th International Conference on Cloud Computing (CLOUD) (pp. 749-752). IEEE.

[39] Khan, N., & War, T. A. A Deep Study on Security Vulnerabilities in Virtualization at Cloud Computing. International Journal of Computer Applications, 975, 8887.

[40] Khodashenas, P. S., Aznar, J., Legarrea, A., Ruiz, C., Siddiqui, M. S., Escalona, E., & Figuerola, S. (2016, July). 5G network challenges and realization insights. In 2016 18th International Conference on Transparent Optical Networks (ICTON) (pp. 1-4). IEEE.

[41] Gui, Y., Siddiqui, A. S., Nicholas, G. S., Hughes, M., & Saqib, F. (2021, April). A lightweight delay-based authentication scheme for dma attack mitigation. In 2021

22nd International Symposium on Quality Electronic Design (ISQED) (pp. 263-268). IEEE.

[42] Niemiec, G. S., Batista, L. M., Schaeffer-Filho, A. E., & Nazar, G. L. (2019). A survey on FPGA support for the feasible execution of virtualized network functions. IEEE Communications Surveys & Tutorials, 22(1), 504-525.

[43] Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C., & Zhang, J. C. (2014). What will 5G be? IEEE Journal on selected areas in communications, 32(6), 1065-1082.

[44] Lal, S., Taleb, T., & Dutta, A. (2017). NFV: Security threats and best practices. IEEE Communications Magazine, 55(8), 211-217.

[45] Gonzalez, A. J., Nencioni, G., Kamisiński, A., Helvik, B. E., & Heegaard, P. E. (2018). Dependability of the NFV orchestrator: State of the art and research challenges. IEEE Communications Surveys & Tutorials, 20(4), 3307-3329.

[46] Han, B., Gopalakrishnan, V., Ji, L., & Lee, S. (2015). Network function virtualization: Challenges and opportunities for innovations. IEEE communications magazine, 53(2), 90-97.

[47] Zhang, Q., & Zhang, Y. Q. (2007). Cross-layer design for QoS support in multihop wireless networks. Proceedings of the IEEE, 96(1), 64-76.

[48] Siaud, I., & Ulmer-Moll, A. M. (2016). Green-oriented multi-techno link adaptation metrics for 5G heterogeneous networks. EURASIP Journal on Wireless Communications and Networking, 2016(1), 1-13.

[49] Kliks, A., Musznicki, B., Kowalik, K., & Kryszkiewicz, P. (2018). Perspectives for resource sharing in 5G networks. Telecommunication Systems, 68(4), 605-619.

[50] Wu, Q., Ding, G., Du, Z., Sun, Y., Jo, M., & Vasilakos, A. V. (2016). A cloud-based architecture for the Internet of spectrum devices over future wireless networks. IEEE access, 4, 2854-2862.

[51] Dharanyadevi, P., & Venkatalakshmi, K. (2016). Proficient routing by adroit algorithm in 5 G-Cloud-VMesh networks. EURASIP Journal on Wireless Communications and Networking, 2016(1), 1-11.

[52] Kokku, R., Mahindra, R., Zhang, H., & Rangarajan, S. (2011). NVS: A substrate for virtualizing wireless resources in cellular networks. IEEE/ACM transactions on networking, 20(5), 1333-1346.

[53] Feng, Z., Qiu, C., Feng, Z., Wei, Z., Li, W., & Zhang, P. (2015). An effective approach to 5G: Wireless network virtualization. IEEE Communications Magazine, 53(12), 53-59.

[54] Qassim, Q.S., Jamil N., Daud M., Patel, A., & Ja'affar, N. (2019). A review of security assessment methodologies in industrial control systems. Information & Computer Security 27(1):47–61

[55] Patel, A., Taghavi, M., Bakhtiyari, K., & Ju´nior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications 36(1):25–41.

[56] Patel, A., Alhussian, H., Pedersen, J. M., Bounabat, B., Ju´nior, J. C., & Katsikas, S. (2017). A Nifty Collaborative Intrusion Detection and Prevention Architecture for Smart Grid Ecosystems. Computers & Security (COSE), 64(C): 92-109.

About the author

Alwi M Bamhdi is an Associate Professor in the Department of Computer Sciences, Umm Al-Qura University, Saudi Arabia. He received his MSc and Ph.D. in Computer Science in 2014 from Heriot-Watt University, UK. His research interests include Mobile Ad Hoc Networks, Wireless Sensor Networks, Information Security, Internet of Things, Cyber Security, Computer Vision, Simulation, and Performance Evaluation.