Scientific Research Publishing

Wireless Sensor Network, 2021, 13, 1-16
https://www.scirp.org/journal/wsn
ISSN Online: 1945-3086
ISSN Print: 1945-3078

Feasibility and Challenges of 5G Network Deployment in Least Developed Countries (LDC)

Ashikur Rahman[1], Salsabil Arabi[1], Raqeebir Rab[2]

[1]Department of Comp. Sci. & Engg. (CSE), Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh
[2]Department of Comp. Sci. & Engg. (CSE), Ahsanullah University of Sci. & Tech. (AUST), Dhaka, Bangladesh
Email: ashikur@cse.buet.ac.bd, salsabilarabishusmi007@gmail.com, raqeebir.cse@aust.edu

How to cite this paper: Rahman, A., Arabi, S. and Rab, R. (2021) Feasibility and Challenges of 5G Network Deployment in Least Developed Countries (LDC). *Wireless Sensor Network*, **13**, 1-16.
https://doi.org/10.4236/wsn.2021.131001

Received: November 25, 2020
Accepted: January 26, 2021
Published: January 29, 2021

Abstract

Growing client population, ever-increasing service demand, and complexity of services are the driving factors for the mobile operators for a paradigm shift in their core technology and radio access networks. 5G mobile network is the result of this paradigm shift and currently under deployment in many developed countries such as United States, United Kingdom, South Korea, Japan, and China—to name a few. However, most of the Least Developed Countries (LDCs) have very recently been implemented 4G mobile networks for which the overall role out phase is still not complete. In this paper, we investigate how feasible it is for LDCs to emphasize on a possible deployment of 5G networks at the moment. At first, we take a holistic approach to show the major technical challenges LDCs are likely to face while deploying the 5G mobile networks. Then we argue that various security aspects of 5G networks are an ongoing issue and LDCs are not technologically competent to handle many security glitches of 5G networks. At the same time, we show that most of the use cases of 5G networks are not applicable in the context of many LDCs (at least at the present time). Finally, this paper concludes that the start of the 5G network deployment in LDCs would take much longer time than expected.

Keywords

5G Network, Least Developed Country, 5G Deployment Challenges, Security

1. Introduction

Internet-based services such as Internet-banking, web-mail, searching, social networks, online chatting and gaming are becoming part of people's day-to-day ac-

tivity. A majority of users access Internet using their mobile phones. A recent study [1] conducted in January 2019 showed that there were 4.4 billion active internet users worldwide and among them, 3.5 billion were social media users. Surprisingly, more than half of all video streaming comes from a mobile device. Since 2011, mobile Internet has grown 504% in daily media consumption. As computation and storage continue to move into the cloud, the number of mobile Internet users is also expected to increase at the same pace. Consequently, mobile Internet service providers are under tremendous pressure in making their systems reasonably scalable and providing guaranteed performance with low latency and high availability. In order to achieve such objectives deployment of 5th generation, mobile networks or simply 5G is inevitable.

Some salient features of 5G networks are high capacity, faster response time with near-zero latency (4 - 5 *ms*), high speed up to 10 Gbps, support of wide range of applications, accommodating 100 times more devices, more software options to upgrade and ubiquitous connectivity, etc. Such handful features do not come without price. 5G deployment is a daunting task—even more challenging for Least Developed Countries (LDCs). According to United Nations (UN), the LDCs are developing countries with a gross national income per capita below US $1035 and have the lowest Human Development Index. We have conducted our research based on the list of LDCs published by UN [2].

Beginning from 1980s, mobile community has received a new generation of technology every decade. The legacy first generation mobile network was deployed in 1980s, 2G in 1990s, 3G and 4G in the decades of 2000 and 2010 respectively. In 2019, the initial 5G services commenced in many developed countries and it is expected to be deployed in a mass scale by 2025. However, the gap between the last two successive generations 4G and 5G seems quite narrow, much narrower in LDCs. Although the deployment of 4G networks started in 2010 in many developed countries, in LDCs the 4G networks were introduced very late in the decade. The implementation timeline of 4G networks for some LDCs is shown in **Table 1**. The deployment pressure of 5G networks will undoubtedly place a heavy burden on LDCs' mobile operators. Needless to say that, the mobile operators have not started realizing Return on Investment (ROI) yet for the 4G networks that they implemented/implementing in LDCs. The situation is even worse in Africa. The mobile operators of most of the African countries are still running 3G [3]. Surprisingly, 4G deployment in Africa is likely to reach only 32 percent in 2020 according to a prediction made by GSMA. On the other hand, the countrywide actual 4G adoption is predicted to be only less than 10 percent in 2020.

This paper is all about a feasibility study of possible 5G mobile network deployment in LDCs. At first, we provide a brief description of new 5G technology. Then, we discuss major technological barriers that will be faced by LDCs while implementing 5G. We show that migration to 5G is not an easy task and includes a number of challenges that are complex, self-interacting and require more

Table 1. 4G deployment time in LDCs.

Country Name	Deployment Year	Company
Afghanistan	2017	AWCC
Nepal	2017	Nepal Telecom
Bangladesh	2018	Teletalk, Gremeenphone, Robi & Banglalink
Bhutan	2016	TashiCell
Uganda	2017	Airtel
Somalia	2017	Somnet
Senegal	2018	Orange

time, funds and resources that LDCs are incapable of providing at present. We also show that most of the over-arching use cases of 5G are not applicable in the current context of LDCs. They require much more advanced market and economic condition which are absent in the LDCs. The prime application of 5G in LDCs will be be enhanced mobile broadband services. The only other game changer use case at present time could be the narrow band IoT or NB-IoT in short. We also show that LDCs are not 5G-ready to handle all its security aspects. Finally, we conclude that beginning of 5G deployment in LDCs will require much longer time than expected.

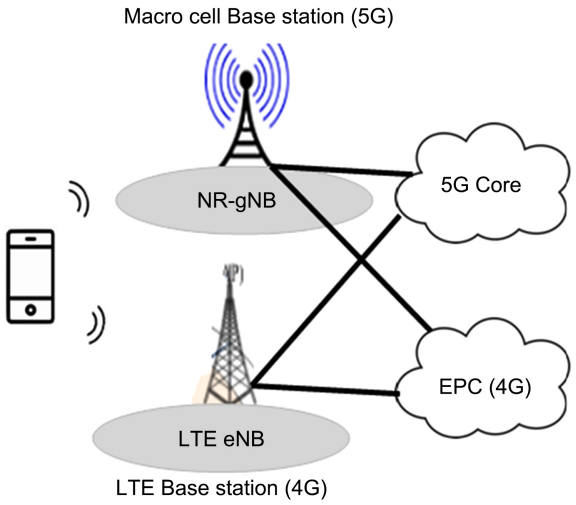
2. A quick overview of 5G architecture

In this section we provide deployment options of 5G and a brief description of its network architecture.

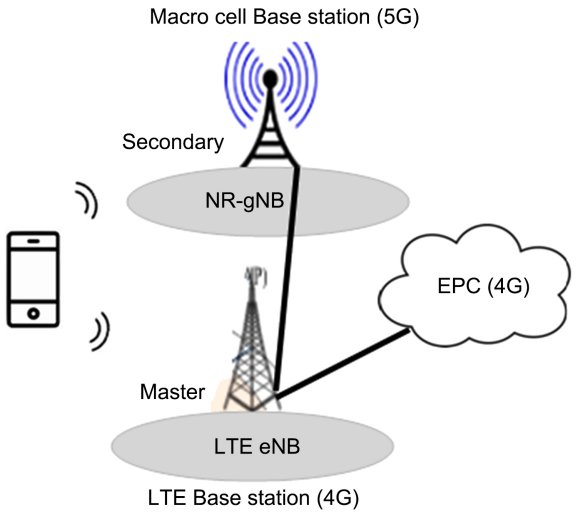
2.1. Deployment Options of 5G

At the beginning, 5G will operate under the umbrella of existing 4G networks. Then it is expected to be fully evolved to a standalone mode when it matures. Some possible co-existence scenarios of 5G with 4G have been shown in **Figure 1**. A detail explanation of all these configurations is as follows.

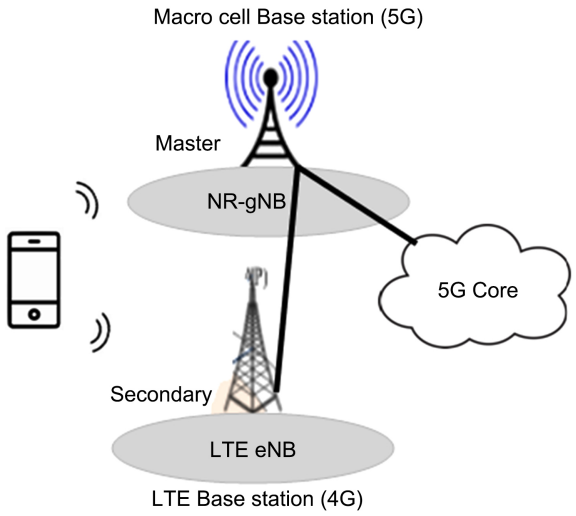
5G technology has two parts, the new radio access interface, and the 5G core. The first configuration option is that the existing 4G network core, *i.e.*, the evolved packet core (EPC) will remain connected with the Long Term Evaluation (LTE) base stations (the so-called eNodeB base stations) and it will be supplemented by the 5G's new radio (NR) technology base stations (called gNodeB base stations, g stands for next generation) as shown in **Figure 1(a)**. The LTE base station will act as a master. A second option might be to replace 4G core with the 5G core as shown in **Figure 1(b)**. The 5G core will remain connected with the gNodeB base stations with new radio (NR) technology. NR base station will act as a master and will be supplemented by existing 4G LTE base station. As a third option there could be a combination of both that will happen at more



(a)



(b)



(c)

Figure 1. How 4G and 5G networks will coexist. (a) 4G eNB master; (b) 5G gNB master; (c) Both eNB and gNB coexists.

mature stage. In this configuration **Figure 1(c)** existing 4G LTE base stations will remain connected with the 4G EPC core (like before). The mobile operators will install additional NR base stations attached to the 5G core. Both will coexist to operate. For all three options, the mobile devices might have single or dual interfaces and connect to either of the base stations.

2.2. 5G Network-Mobile Network Architecture

Two major components of 5G are discussed below in brief. More details can be found in [4] [5] and from many other resources available on the web.

Radio access network (RAN). RAN in 5G shall consist of small cells, macro cells, towers, in building and street-side hotspots and many more. Its purpose is to allow mobile devices to become attached with the main core. The 5G macro cell contains gNodeB base stations with new radio technology and covers more wider area. The new radio in 5G is a more flexible version of LTE radios which are also software configurable supporting much higher bit rates. However, it is still OFDM based. In order to provide a continuous connection, a novel concept of small cells has been introduced in 5G networks. Small cells, containing mini base stations, operate at the new millimeter wave (mmWave) frequencies. Consequently, their connection range is very short (typically 10 m) and coverage area is much smaller. But they are distributed in clusters to complement the macro cells.

The new radio technology of 5G Macro cells contains MIMO (multiple input, multiple output, sometimes called massive MIMO) antennas consisting of a large number of multiple elements or connections so that they can operate in full-duplex mode. As a result, the system is highly scalable accommodating more users in parallel.

The core network. Like previous generations, the 5G core is the mobile exchange network managing mobile voices. It also contains the data network managing mobile data and internet connections and also has been redesigned to integrate with cloud-based services. Interestingly, 5G core contains distributed servers spread over large geographic regions so that content can be accessed locally and in a distributed way near the client's premises. Distributed servers also enable edge computing so that majority of data can be processed at the client's end without flooding the core network.

Two other important features network slicing and network function virtualization are also handled by 5G core. Through network slicing several independent virtualized logical networks can be created on top of the same physical network infrastructure. Then network slices can be assigned dedicatedly to an application or to a user. In order to select resources to fulfill service demands in an optimal manner, orchestration is used [6]. The orchestration functions perform user-specific service demand validation and resource configuration. Each user receives a unique set of network resources and topology depending on the need of the application. Network slicing plays a crucial role in supporting mas-

sive amounts of IoT connectivity [7]. On the other hand, network function virtualization decouples network functions such as domain name services, encryption or firewall running on dedicated networking elements in customer premises and moves the functions to run on virtual servers in the cloud.

3. Technical Aspects and Challenges

Despite a handful of features and their potential benefits, there exist significant technical challenges to implement 5G. Some of the key challenges are listed below.

Spectrum allocation. In order to achieve higher data rates and massive network capacity, 5G requires a high amount of spectrum. The requirement includes a low frequency band of less than 1 GHz, a mid-frequency band (in 2.3 - 3.5 GHz range) for its macro cells, and a high frequency band (mmWave in 26 - 100 GHz range) for its micro cells. A typical current spectrum usage in LDCs has been shown in Figure 2. Note that, a handful of clean-ups, harmonization and policy level interventions are required to make the necessary spectrum available for 5G which might create some additional challenges. For example, if a chunk of spectrum in the required band is already sold out to a third party for other purposes (such as for implementing Wi-Max) then a buy-back option is needed which may not be feasible always. It might trigger some legal issues. Also, some part of the spectrum could be already assigned to government organizations for which the regulatory authority must go through a very hard negotiation process to recover.

Spectrum costs. Another concern is spectrum prices. A recent study shows that spectrum prices in LDCs is, on average, more than three times higher than that of developed countries [8]. Thus, the cost of spectrum could be a major factor that will make a difference in 5G roll-out from country to country.

Lack of infrastructures. Access to infrastructure is one of the critical aspects to ensure 5G coverage and capacity [9]. Infrastructure includes towers, antenna etc to host base stations and accessories needed for their inter-connectivity. 5G operators consider fiber connectivity as an important factor for the back-haul

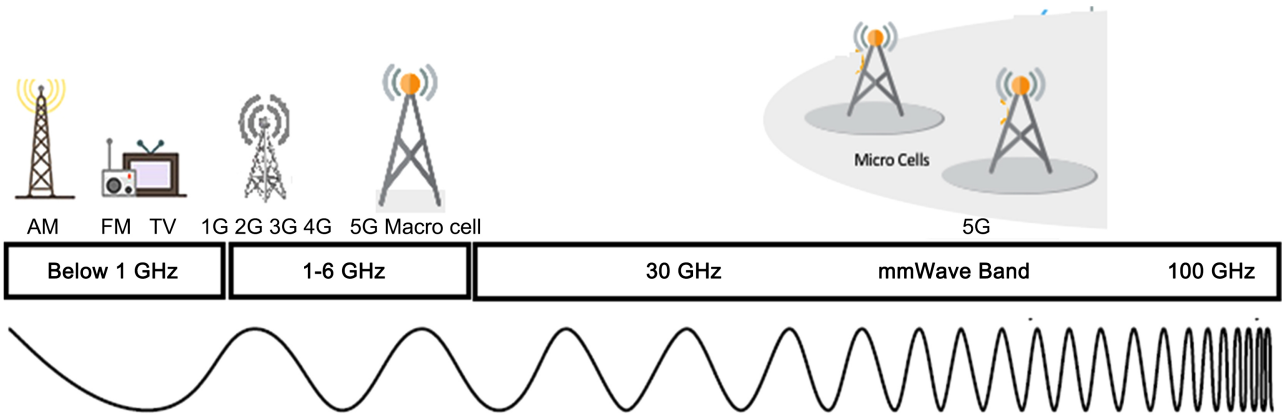


Figure 2. Spectrum allocation.

portion of the network to achieve massive capacity. Currently most of the base stations in 4G are not connected using fiber. Developing optical fiber infrastructure is expensive and it comes with high maintenance costs too [10]. For this reason, mobile operators often use microwave radio spectrum to connect back-hauls. But microwave communication requires a line-of-sight connection which can potentially be an issue.

Cost of increased network density. Even if the spectrum is abundant the achievable network capacity shall remain low if the network density is lower. The density of a network is determined by the number of base stations placed over a terrain against the population. A higher density requires higher cost. Lower density is a typical phenomenon in Latin America, Africa, and India. In order to support the cluster of micro cells the density of 5G networks must be much higher. This requirement creates an additional challenge of funding and building adequate base stations to support necessary coverage of 5G networks [11].

Dynamic spectrum sharing. One of the distinct features of 5G is the use of cognitive radios. This type of radios can opportunistically detect and use available channel in the neighborhood. But this also requires a spectrum sharing policy to be established among the mobile operators first, otherwise detected opportunities cannot be used due to payment issue. Regulatory authorities in LDCs usually do not allow spectrum sharing between operators in a fear of possible revenue losses.

4. 5G Use Cases and Applicability

In this section we discuss use cases and their possible applicability in the context of LDCs.

4.1. Use Cases

The earlier generations of mobile networks were intended solely for humans. 2G was mainly used for phone calls and text messaging between people. 3G/4G is the generation of smart phones where people use the mobile network for data services besides usual phone calls/text messaging. In 5G, humans are no more the sole users—in fact humans are becoming more and more minority users [4] in 5G and subsequent generations to come. There will be many different types of users and applications using the 5G networks. The use cases of 5G can be broadly divided into three major categories:

1) Enhanced Mobile Broadband (eMBB): eMBB has been designed to provide humans' voice, data and text messaging services but this time at a greater speed (10 Gbps) highly suitable for streaming 3D videos, HD TV, playing or working in the cloud, streaming live events, and much more.

2) Massive Machine Type Communication (mMTC): mMTC has been designed to support hunderds of billions of IoT devices to remain connected not over Wi-fi or bluetooth but through mobile networks [4]. Some applications of

mMTC are vehicle-to-vehicle communications, smart cities with asset tracking, smart agriculture, environment monitoring, smart water management, waste management, smart grid, energy monitoring, smart home, remote monitoring etc. Small machines such as sensors, water meters, smoke detectors, bicycles, buses, alarms etc. will be regarded as the users.

3) Ultra Reliable Low Latency Communication (URLLC): The eMMB and mMTC have been designed solely for humans and machines respectively but URLLC has been designed for human-to-machine interaction. This communication is supposed to be with near-zero latency and near-zero packet losses supporting mission critical applications such as autonomous vehicles, augmented virtual reality, remote patient surgery using robots etc.

4.2. Applicability of Use Cases in the Context of LDCs

Among three use cases, it is highly likely that eMBB that supports fixed wireless access for homes and enhanced mobile broadband services will be the prime applications of 5G in LDCs. Users in LDCs will mostly perform data access, downloading and streaming content. Moreover, 5G phones, tablets and hotspots will remain at an unaffordable price for many years in LDCs as users have very low average income. Therefore, in order to utilize the benefits of 5G core, users in LDCs will still continue to use their 4G phones and 4G/5G base stations are likely to coexist for many years.

Some use cases require well established transport or health sectors and/or advanced market structures. For example, autonomous vehicles and remote-controlled robotic surgery under URLCC are clearly futuristic applications which may not become feasible for a very long time in LDCs.

Massive machine to machine communications (the second use case) depends on socio-cultural aspects of a country. For example, in order to understand the actual value of smart cities with asset tracking, smart waste management, remote elderly people monitoring etc., the social structure needs to be much stronger, standard of living has to be very high and at the same time people should be well educated. All of these conditions are mostly absent within the social structure of LDCs.

For some other use cases the LDCs are not 5G-ready yet. Such applications include autonomous vehicles and robotic surgery. These are not applicable in the context of LDCs due to unavailability of supportive economic infrastructure.

Only prospectus 5G use case is the Narrow Band IoT or NB-IoT which is likely to be a game changer in the context of LDCs [3]. NB-IoT is one of the prime Low Power Wireless Access (LPWA) technologies that can support end devices battery for more than 10 years especially in underground, tunnels, indoor shopping malls, basement parking lots, or in rural areas. NB-IoT can be incorporated in static devices like utility meters, street lights, parking meters, pipelines, and in mobile elements like vehicles, pets, containers and can easily be used for package tracking or inventory monitoring [3]. Bangladesh and Sri-Lanka have already

started building NB-IoT applications. For developing countries, NB-IoT implementation is easier as they have rolled out 4G very late and newer version of 4G devices have the required support for NB-IoT.

5. Security Aspects and Challenges

In this section we present a brief discussion on the major security threats of 5G network. Then we show how LDCs are incompetent to handle those security threats.

5G network has its own security challenges arising from its adopted advanced technologies to fulfill its envisioned goals. In this study, we mostly emphasize on the security threats revealed by three major technologies incorporated by 5G namely Software Defined Networking (SDN), Network Function Virtualization (NFV), and Internet of Things (IoT).

5.1. Security Challenges of SDN

SDN establishes centralized and programmable control plane by decoupling it from the data plane. Independent control and data plane create opportunities along with some security loopholes. The control information traffic passing through the controller and data plane channel can be a potential option for denial-of-service (DoS) attacks [12] making the network resources unavailable to the users. The data plane itself can be exploited by attackers to produce counterfeit flow requests having serious consequences on the network [13]. The controller acts as a bottleneck for the network during saturation attack due to centralized network control [14]. In addition, centralized controller can be manipulated to generate DoS attacks and data theft making it an attractive target to attackers [15].

Hussain *et al.* accused the programmability of SDN for providing malware an open ground for malicious behaviors including Spoofing and Man-In-The-Middle (MITM) attacks [16]. They further discussed another attack called controller hijacking, which enables an attacker to exercise unwarranted control over the controller while providing scope to collect sensitive information such as passwords. The channel between the controller and the switches is established over a non-secure connection which is highly vulnerable to MITM attacks [17]. It is quite possible to compromise the controller and manipulate the network according to the attacker's wish through MITM attacks. Due to ubiquitous connectivity, MITM attacks will have even far-reaching effects as it can exploit real-time transaction and data transfer.

Malicious applications and APIs exposed to unintended software can knock the complete network down and create a significant damage. The open-source implementation of OpenFlow, which is the communication protocol of SDN, provides attackers opportunities to identify possible vulnerabilities. Using Host Location Hijacking Attack, an attacker can hijack the location information of a server by using the Host Tracking Service of OpenFlow [18]. Antikainen *et al.*

asserted in [19] that in the absense of Transport Layer Security (TLS) encryption with OpenFlow, the attackers can create fake virtual switches to deploy Topology Spoofing Attacks along with launching state spoofing attacks using a compromised switch. The authors further stated that an attacker can use virtual and compromised switches to create alternative paths, unwarranted congestion as well as reserving bandwidth for the attacker himself.

5.2. Security Challenges of NFV

NFV opens promising scopes to address dynamic user requirements, service agility, and scalability. But these benefits carry along some security challenges. It provides programmable orchestration and interaction with the infrastructure using APIs. These APIs are potential sources of security threats [20]. In a cloud environment, Virtual Network Functions (VNFs) may lead to security threats like confidential data leakage, malicious loops, network failures, and abuse of hypervisor, one of the architectural components of NFV [21]. Hypervisor domain can face unauthorized access and data leakage [22]. Lal, S. *et al.* [23] presented existing security threats on NFV and spotted various security attacks on hyprevisor including Virtual Machine (VM) operating system manipulation, unauthorized data transfer, and retrieval or data destruction which cause other vulnerabilities to rise exponentially. They also mentioned about VM escape attack which can be deployed if there is lack of proper isolation between hypervisor and VNFs. Using the aforementioned attack, attackers can even exploit virtual firewalls. The complexity and dynamicity of the virtual environment make VNFs more prone to configuration error. The breaking of virtual machine is critical as it is quite impossible to detect. Virtualization also raises authenticity issue as once a virtual machine is duplicated, the original machine does not exist anymore. VNFs are highly at risk of DoS attacks, flood attacks, configuration attacks and cloud and VM specific attacks [14]. Inefficient design and deployment of the application can lead to buffer overflow attacks. The vulnerability of VNFs to side-channel attacks, distributed denial-of-service (DDoS) attacks [24], and other cyber-attacks puts the confidentiality and integrity of the users at stake.

5.3. Security Challenges of IoT

Connectivity of massive number of heterogeneous devices to the internet poses serious security challenges along with making the deployment of security mechanisms difficult to scale. IoT devices are vulnerable to traditional attacks such as MITM attacks, password cracking along with DoS attacks and disruption attacks. Sensors of IoTs can be victims of spoofing attacks, replay attacks as well as system capturing attacks where attackers try to gather and manipulate data by accessing sensors [25]. Communication links can be exploited using sniffing and tampering attacks and information and traffic might get hacked, menacing the privacy of numerous connected devices. Real-time data transmission among heterogeneous IoT devices can face congestion problem due to lack of data rate

compatibility between sender and receiver devices [26]. The heterogeneity of connected devices makes the private data unprotected due to the lack of proper security infrastructure. The absence of cryptographic integrity protection for user data plane provides additional security threats to IoT devices [27]. The exponential growth of IoT devices will make DDoS attacks more catastrophic and way more easier to arrange [28].

5.4. Competence of LDCs towards 5G Security

While 5G network provides a wide range of security threats, LDCs hardly have enough capacity to defend against those. Incapability of LDCs in tackling the security breaches in other domains has been seen in the past. For example, the incident of Bangladesh Bank Robbery [29] in 2016, known as Bangladesh Bank cyber heist is a good example of the cyberattacks that went undetected. During this attack, security hackers illegally transferred $101 million from Bangladesh Bank. Clearly this type of incident questions the LDCs' expertise in tackling advanced security breaches of 5G network. LDCs' incompetency in defending against advanced security threats can be pictured due to the following key reasons.

Lack of security experts. LDCs have a large void in number of skilled workforces as their education systems are not sufficiently funded to produce such [30]. In 2012, the total public expenditure on education in developed countries was approximately 5.98 percent of GDP whereas in LDCs, the percentage was only 3.6 percent of GDP [31]. In 2016, this expenditure increased to 7.16 percent in the developed countries whereas it remained almost at the same level of only 3.81 percent in LDCs [32]. Such a lower investment in education cannot produce efficient IT workers as well as security experts making the sustenance of 5G network-like new technologies even harder. The governments' sub-optimal investment in training of staffs, low investment in research and development (R&D) are also responsible to a greater extent. In order to handle the security challenges of 5G, well-trained security experts have no substitute. It is not affordable and sustainable to import skilled manpower and IT personnel always.

Lack of strong infrastructure. Besides competency, protecting 5G network from security challenges require hardened infrastructure and adequate legal and regulatory framework. Sub-standard hardware and insufficient equipment can create a barrier in developing complex and secure network infrastructures. Due to economic constraints, LDCs cannot even invest enough to import sophisticated security equipment.

Poor funding in R&D. LDCs do not have sector specific Research and Development (R&D) programs. In LDCs, the proportion of government expenditure on R&D is less than 1 percent of GDP [33]. Therefore, they lack in skills and scopes to develop their own software and hardware and always need to import from abroad. Handling the security issues of these exogenous tools is even harder for them as they have lack of field specific knowledge and skill.

Missing security education. In developed countries, an exhaustive range of IT security education is included in the curriculum of high school, undergraduate as well as graduate studies. For example, USA has created the National Initiative for Cybersecurity Education (NICE) for the betterment of long-term cybersecurity posture. Several universities have introduced cybersecurity programs which are supported by skilled workforce. But in LDCs, IT security education and awareness is not included in the academic curriculum. Due to lack of concern, resources, and will power, they do not run IT and security education program. According to [34], in Ecuador, which is a moderately developed country, on average, 30 percent university academic curriculum offer no course on cybersecurity, 50 percent offer one course and only 20 percent offer two courses and students tend to avoid these courses as they are optional in most of the universities. As a result, LDCs fail to produce skilled manpower to prevent security attacks against a nation's critical infrastructure like 5G network.

Resistance to changes. Tauray *et al.* conducted an empirical study on one of the LDCs namely Gambia and identified 43 ICT barriers in developing countries [35]. According to the authors, people are always resistant to changes and reluctant to adapt new technologies which are a critical obstacle in establishing any new technology in any country. According to Mushfoq Mobarak, a development economist at Yale SOM, highlighted three key constraints that affect technology adaption in poor countries the most: information failure, cost and risk aversion [36]. According to Richardson [37], which was based on the technology adoption scenario of a least developed country Cambodia, people face difficulty in finding advantages of adopting ICT and therefore, are reluctant to adopt new technologies. Establishing 5G in LDCs, where more than 75 percent of the population still live in poverty, will not be much different from that.

6. Conclusion

We present a short survey on the feasibility of 5G network deployment in the current context of Least Developed Countries (LDCs). While implementing 5G, LDCs are likely to face several technical, and security challenges. Some of the technical challenges are creating contiguous spectrum out of scatteredly assigned spectrum, high spectrum prices, poor mobile network infrastructure, lack of policy in dynamic sharing of spectrum, etc. Handling these issues needs a huge amount of economic resources as well as skilled manpower. Some of the security challenges are DoS/DDoS attacks, MITM attacks, exploiting existing loopholes in open-source software—all inherited from SDN. There are some NFV related threats such as confidential data leakage, malicious loops, network failures and abuse of hypervisor by malicious VMs. And then the support of massive IoT opens up major security threats like spoofing attacks, replay attacks, system capturing attacks, sniffing and tampering attacks, etc for which defense mechanisms are extremely difficult to scale due to massiveness in a number of devices. In order to maintain the security of SDN and prevent DoS/DDoS attacks, it is re-

quired to improve the security of centralized control plane along with controlling frequent access to the SDN. The security of the shared channel between data and control plane needs to be increased to handle MITM attacks. The NFV security can be increased by using firewalls and message encryption. Researchers as well as some other organizations are dedicatedly looking for possible countermeasures to overcome these challenges and propose several solutions as well. However, LDCs do not have enough expertise to handle 5G security challenges. Neither do they have enough funds to create skilled security professionals. The major use cases of 5G are not applicable in the present context of LDCs as they lack advanced market structures and their economic condition does not support many possible applications. Overall, the beginning of 5G deployment is likely to take more time than expected and once deployed, its countrywide actual adoption will take even much longer time span.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] What Percentage of Internet Traffic Is Mobile in 2020?
https://tinyurl.com/y5tp47ak

[2] Ldc List by United Nations.
http://www.un.org/development/desa/dpad/least-developed-country-category/ldcs-at-a-glance.html

[3] NB-IoT: The IoT Game Changer.
https://www.linkedin.com/pulse/nb-iot-iot-game-changer-reduan-hasan-khan-phd?trk=relatedarticeNB-IoT

[4] 5G Core Network Architecture.
https://www.youtube.com/watch?v=z7XqOUOmmWw

[5] 5G Explained—How 5G Works.
http://www.emfexplained.info/?ID=25916

[6] Ordonez-Lucena, J., Ameigeiras, P., Lopez, D., Ramos-Munoz, J.J., Lorca, J. and Folgueira, J. (2017) Network Slicing for 5g with SDN/NFV: Concepts, Architectures, and Challenges. *IEEE Communications Magazine*, **55**, 80-87.
https://doi.org/10.1109/MCOM.2017.1600935

[7] Foukas, X., Patounas, G., Elmokashfi, A. and Marina, M.K. (2017) Network Slicing in 5g: Survey and Challenges. *IEEE Communications Magazine*, **55**, 94-100.
https://doi.org/10.1109/MCOM.2017.1600951

[8] Developing Countries Are Hard Hit by High Spectrum Prices.
https://www.gsma.com/spectrum/resources/spectrum-prices-developing-countries

[9] 5G in Bangladesh: Opportunities & Challenges.
https://www.linkedin.com/pulse/5g-bangladesh-opportunities-challenges-reduan-hasan-khan-phd

[10] Indoria, S. (2020) Deployment of 5G Networks Challenges for Developing Countries. In: *ICT Analysis and Applications*, Springer, Berlin, 255-262.
https://doi.org/10.1007/978-981-15-0630-7_25

[11] Holma, H., Luostari, R., Reunanen, J. and Thepchatri, P. (2019) Deployment Aspects. In: Holma, H., Toskala, A. and Nakamura, T., Eds., 5*G Technology*: 3*GPP New Radio*, John Wiley & Sons Ltd., Hoboken, Chapter 8, 187-212. https://doi.org/10.1002/9781119236306.ch8

[12] Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M. and Gurtov, A. (2017) 5g Security: Analysis of Threats and Solutions. 2017 *IEEE Conference on Standards for Communications and Networking* (*CSCN*), Helsinki, 18-21 September 2017, 193-199. https://doi.org/10.1109/CSCN.2017.8088621

[13] Seungwon, S., Yegneswaran, V., Porras, P. and Gu, G.F. (2013) AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software Defined Networks. *The ACM Conference on Computer and Communications Security*, Berlin, 4-8 November 2013, 413-424. https://doi.org/10.1145/2508859.2516684

[14] Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M. and Gurtov, A. (2018) Overview of 5g Security Challenges and Solutions. *IEEE Communications Standards Magazine*, **2**, 36-43. https://doi.org/10.1109/MCOMSTD.2018.1700063

[15] Kreutz, D., Ramos, F. and Verıssimo, P. (2013) Towards Secure and Dependable Software-Defined Networks. *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, Hong Kong, 16 August 2013, 55-60. https://doi.org/10.1145/2491185.2491199

[16] Hussein, A., Chaddad, L., Adalian, N., Chehab, A., Elhajj, I. and Kayssi, A. (2019) Software-Defined Networking (SDN): The Security Review. *Journal of Cyber Security Technology*, **4**, 1-66. https://doi.org/10.1080/23742917.2019.1629529

[17] Brooks, M. and Yang, B.J. (2015) A Man-in-the-Middle Attack against Open Daylight SDN Controller. *Proceedings of the* 4*th Annual ACM Conference on Research in Information Technology*, Chicago, 30 September-3 October 2015, 45-49. https://doi.org/10.1145/2808062.2808073

[18] Hong, S., Xu, L., Wang, H.P. and Gu, G.F. (2015) Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures. *Proceedings* 2015 *Network and Distributed System Security Symposium*, San Diego, 8-11 February 2015, 1. https://doi.org/10.14722/ndss.2015.23283

[19] Antikainen, M., Aura, T. and Sarela, M. (2014) Spook in Your Network: Attacking an SDN with a Compromised Openflow Switch. *Proceedings of the Nordic Conference on Secure IT Systems*, Vol. 8788, 229-244. https://doi.org/10.1007/978-3-319-11599-3_14

[20] Hawilo, H., Shami, A., Mirahmadi, M. and Asal, R. (2014) NFV: State of the Art, Challenges, and Implementation in Next Generation Mobile Networks (VEPC). *IEEE Network*, **28**, 18-26. https://doi.org/10.1109/MNET.2014.6963800

[21] Monshizadeh, M., Khatri, V. and Gurtov, A. (2016) NFV Security Considerations for Cloud-Based Mobile Virtual Network Operators. *IEEE*, *the* 24*th International Conference on Software*, *Telecommunications and Computer Networks*, Split, 22-24 September 2016, 1-5. https://doi.org/10.1109/SOFTCOM.2016.7772161

[22] Yang, W. and Fung, C. (2016) A Survey on Security in Network Functions Virtualization. 2016 *IEEE NetSoft Conference and Workshops*, Seoul, 6-10 June 2016, 15-19. https://doi.org/10.1109/NETSOFT.2016.7502434

[23] Lal, S., Taleb, T. and Dutta, A. (2017) NFV: Security Threats and Best Practices. *IEEE Communications Magazine*, **55**, 211-217. https://doi.org/10.1109/MCOM.2017.1600899

[24] Reynaud, F., Aguessy, F., Bettan, O., Bouet, M. and Conan, V. (2016) Attacks against Network Functions Virtualization and Software-Defined Networking:

State-of-the-Art. 2016 *IEEE NetSoft Conference and Workshops* (*NetSoft*), Seoul, 6-10 June 2016, 471-476. https://doi.org/10.1109/NETSOFT.2016.7502487

[25] Chasaki, D. and Mansour, C. (2015) Security Challenges in the Internet of Things. *International Journal of Space-Based and Situated Computing*, **5**, 141-149. https://doi.org/10.1504/IJSSC.2015.070945

[26] Javaid, N., Sher, A., Nasir, H. and Guizani, N. (2018) Intelligence in IoT-Based 5g Networks: Opportunities and Challenges. *IEEE Communications Magazine*, **56**, 94-100. https://doi.org/10.1109/MCOM.2018.1800036

[27] Shah, Y., Chelvachandran, N., Kendzierskyj, S., Jahankhani, H. and Janoso, R. (2020) 5G Cybersecurity Vulnerabilities with IoT and Smart Societies. In: *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, Springer, Berlin, 159-176. https://doi.org/10.1007/978-3-030-35746-7_9

[28] Fonyi, S. (2020) Overview of 5G Security and Vulnerabilities. *The Cyber Defense Review*, **5**, 117-132.

[29] Hacked: The Bangladesh Bank Heist. https://www.aljazeera.com/programmes/101east/2018/05/hacked-bangladesh-bank-heist-180523070038069.htm

[30] Granville, B., Leonard, C. and Manning, J. (2000) Information Technology and Developing Countries: Potential and Obstacles.

[31] Total Public Expenditure on Education in Year 2012. http://hdr.undp.org/en/content/expenditure-education-public-gdp

[32] Total Government Expenditure on Education in Year 2016. https://ourworldindata.org/financing-education

[33] Closing the Technology Gap in Least Developed Countries. https://www.un.org/en/chronicle/article/closing-technology-gap-least-developed-countries

[34] Catota, F.E., Morgan, M.G. and Sicker, D.C. (2019) Cybersecurity Education in a Developing Nation: The Ecuadorian Environment. *Journal of Cybersecurity*, **5**, tyz001. https://doi.org/10.1093/cybsec/tyz001

[35] Touray, A., Salminen, A. and Mursu, A. (2013) ICT Barriers and Critical Success Factors in Developing Countries. *Electronic Journal of Information Systems in Developing Countries*, **56**, 1-17. https://doi.org/10.1002/j.1681-4835.2013.tb00401.x

[36] What Keeps the Poor from Adopting New Technology? https://insights.som.yale.edu/insights/what-keeps-the-poor-from-adopting-new-technology

[37] Richardson, J.W. (2011) Challenges of Adopting the Use of Technology in Less Developed Countries: The Case of Cambodia. *Comparative Education Review*, **55**, 8-29. https://doi.org/10.1086/656430

List of Abbreviations

LDC—Least Developed Country,
NFV—Network Function Virtualization,
SDN—Software Defined Network,
VNF—Virtual Network Function,
MITM—Man-in-the-Middle,
DoS—Denial of Service,
LTE—Long Term Evaluation,
VM—Virtual Machine,
RAN—Radio Access Network,
MIMO—Multiple Input, Multiple Output