International Journal of Networks and Communications 2019, 9(2): 82-88
DOI: 10.5923/j.ijnc.20190902.03

Integration of SDN and 5G and Its Related Challenges and Security Issues

Nilofer Fatma, Jihad Qaddour*

School of Information Technology, Illinois State University, Normal, IL USA

Abstract The 5G technology is presently in its early research stages, so researches are currently underway exploring different architectural paths to address their key drivers. SDN techniques have been seen as promising enablers for the future networking, is likely to play a crucial role in the design of 5G wireless networks. A critical understanding of this emerging paradigm is important to understand that address multiple challenges and security issues of the future SDN-enabled 5G technology. This paper discusses the challenges and security issues that comes up by integrating SDN and 5G technology and proposed some solutions to overcome it.

Keywords SDN, 5G, Security, QoS

1. Introduction

The 5G technology is presently in its early research stages, so research is currently underway exploring different architectural paths to address their key drivers. Whereas, SDN technology have been seen as promising enablers for this vision of carrier networks, which will likely play a crucial role in the design of 5G wireless networks. A critical understanding of this emerging paradigm is necessary to address the multiple challenges and security issues in the future SDN-enabled 5G technology. With the integration of SDN and 5G technology, the complexity has been increased due to the hybrid infrastructure which may to leads to various challenges and security requirements that must be satisfied. Even as a leading SDN technology, the application of OpenFlow in the next generation of mobile network is still a challenging problem [2]. The advantage of SDN in 5G networks lies in its ability to provide new capabilities like automation and creating new services on top of the virtualized resources, in secure and trusted networks. SDN enables the separation of the control logic from vendor-specific hardware to open and vendor-neutral software controllers. Thus, it enables implementing routing and data processing functions of wireless infrastructure into software packages in general purpose computer or even in the cloud [2].

This paper is organized in four sections: Section I gives the general introduction of the SDN architecture framework, Section II gives the description of 5G architecture, Section III discusses how SDN can be used in 5G architecture, Section IV describe the security challenges and proposed solutions for 5G leveraging SDN, Section V gives the conclusion, Section VI presents future intended research.

* Corresponding author:
jqaddou@ilstu.edu (Jihad Qaddour)
Published online at http://journal.sapub.org/ijnc

2. SDN Architecture

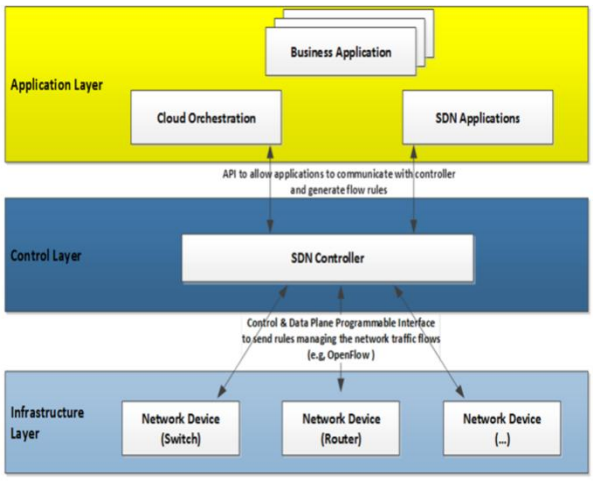

Figure 1. SDN architecture

The SDN architecture consists of the following key planes as shown in Figure 1.

• *Data plane/infrastructure layer:*

The Data Plane layer is also known as a Resource layer or Infrastructure layer, it is the bottom layer in the SDN architecture as shown in Figure 1. It primarily consists of a data forwarding unit including physical switches and virtual

switches for exchanging and forwarding data packets to the SDN controller. We also categorize the physical mobile terminal as belonging in the data plane. The networking devices in the data plane layer perform simple forwarding functions, without embedded software to make autonomous decisions.

- *Control plane:*

The control layer consists of a server or set of servers known as SDN controllers that providing centralized control. The Open API (Application Program Interface) enables open switches data forwarding functions to realize the state collection and centralized control of the data plane. The controller can be seen as a *Network Operating System (NOS),* it provides essential services, common application programming interfaces, and abstraction of lower level network devices to developers.

- *Application layer:*

It is the upper layer that provides various applications to end-users, such as mobile management, security application, network virtualization, etc. This layer consists of applications and services that define, monitor and control network resources. The mobile terminal applications are also categorized into this plane. The applications at this layer interact with SDN controller via API's, to automatically customize the behavior and properties of network resources. The programming of an SDN application layer make use of the abstracted view of the network resources which is provided by the SDN controller through API's.

The primary idea behind the evolution of SDN technology is to move the control plane outside the switches and enable external control of data through a logical software entity called controller. SDN provides simple abstractions to describe the components, the functions they provide, and the protocol to manage the forwarding plane from a remote controller through secure channel. The abstraction provided by the SDN controller, captures the common requirements of forwarding tables for a majority of switches and their flow tables. This centralized up-to-date view makes the controller suitable to perform network management functions while allowing easy modification of the network behavior through the centralized control plane [2].

SDN is a modern approach to networking that eliminates the complex and static nature of legacy distributed network architectures through the use of a standards-based software abstraction between the network control plane and underlying data forwarding plane, including both physical and virtual devices. The ultimate goal of SDN is to create automated network that does not need any design or adjustments of the administrator interference, so, the network can be implemented through a fully automated administration. The administrators can manage the network through the controller plane more easily with dictating the required policy, while they have a fully function monitoring over the network.

3. 5g Architecture

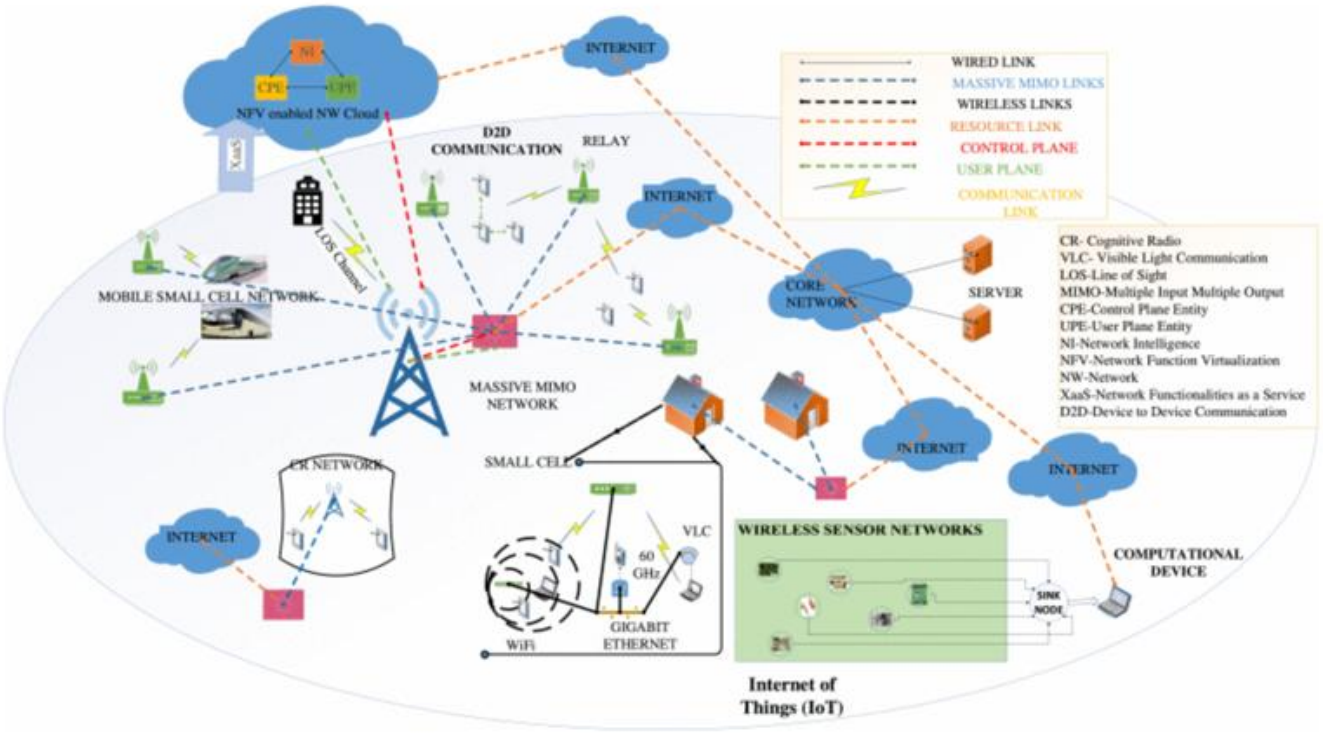

Figure 2. 5G Architecture [5]

Research and development activities on 5G technologies have attracted lots of interest in both academia and industry worldwide over the last several years. The 5G technology is being seen as user-centric concept instead of operator-centric as in 3G and service-centric as seen for 4G. In 5G, mobile terminals will be able to combine multiple incoming flows from different technologies. It aims to provide single user terminal that can cooperate in different wireless networks and overcome the design problem of power-consumption and cost old mobile terminals. The new 5G technology should be enable the development and exploitation of massive capacity as well as connectivity of complex and powerful heterogenous network. The new infrastructure should be able to handle the complex context of operations to support diverse set of new as well as yet unforeseen services, users and applications. It should be able to flexible and scalable for wildly different network deployment scenarios, in an energy efficient and secure manner.

5G networks will not be based on routing and switching technologies anymore, instead it will be more open and flexible, and will be able to evolve more easily than the traditional networks. They will be able to provide convergent network communication across multi-technologies networks such as packet or optical networks and provide open communication system to cooperate with satellite systems, cellular networks, clouds, data-centers, home gateways, and many more open networks and devices. 5G systems will be autonomous and sufficiently able to adapt their behavior depending in the user's requirements to handle application-driven networks in dynamic and versatile environments [2]. Hence, one of the key requirements of future networks will be security, resiliency, robustness and data integrity.

4. 5G Leveraging SDN

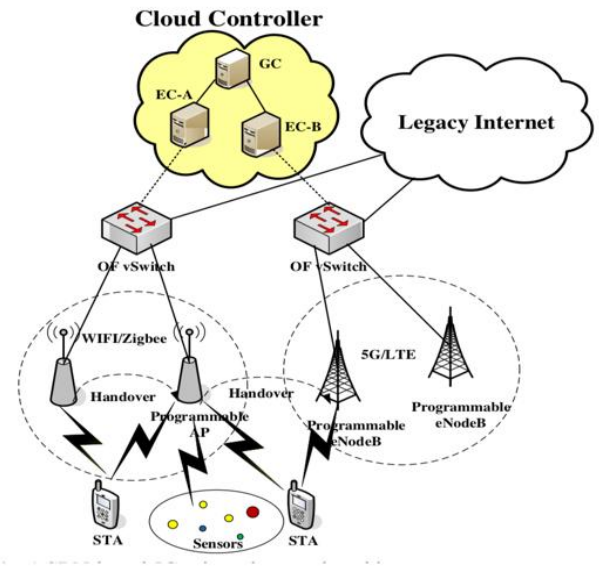

Figure 3. Architecture of 5G leveraging SDN [1]

With the advent of intelligent network architecture such as SDN, hardware constraints have been minimized. SDN provides an abstract layer where it moved the lower level functions to a normalized control plane and manages all the network behavior by the use of API's. As a result, the network administrators can provide services through the network irrespective of the hardware components.

By leveraging 5G along with SDN we are trying to push the limits of what is achievable and increase the functionality by taking the advantages of both the technologies to enhanced performance. It can provide better data flows in the control plane as data moves across the 5G network, as well as network bandwidth and latency can be minimized greatly. Hence, by using SDN in 5G networks, we can automate and manage network redundancy as well as circumnavigating major outages by determining optimal data flows in real time from the centralized control plane. The infrastructure of the 5G networks will be based on SDN, which provides the communication between the applications and services in the cloud and user's mobile terminal. This will allow the network to be managed on the real-time needs and scale dynamically, and it will have benefit from resource virtualization. Although SDN has several advantages such as resource sharing and session management but the main limitation of using SDN for 5G is the computing capabilities and resources of mobile devices. Since, mobile users send request over and over to the embedded controller for flow rules in OpenFlow messages, the overhead increases more significantly on the controller. Hence, further researches are required on leveraging SDN for 5G networks. The Operation and Management (OAM) of wireless mobile network within 5G can be implement using SDN which will increase the performance by constant optimization, fast-failure recovery, fast adapted in changes in the network loads, self-network organization and fast configuration. It also reduces the bottlenecks of the network and enable debugging and troubleshooting of the control traffic.

To increase the capacity of 5G systems, SDN can provide solutions to overcome the limitations of multi-hop wireless networks [6]. Leveraging SDN for 5G can provide high capacity by implementing advance caching techniques to store data at the edge network. Hence, by implementing SDN for 5G, gives greater freedom for users/providers to balance operational parameters such as Network resilience, service performance and QoE. OpenFow can provide rapid response to the mobile subscribers across different technologies without disruptions in the service. Additionally, along with the advantages that SDN can provide in 5G technology such as flexibility, supporting many subscribers, frequent mobility, real-time adaption and so on, it also increases the security challenges for future 5G architecture.

5. Security Challenges

The basic properties of a secure communications in a network includes: confidentiality, integrity, availability of

information/data or resources, authentication and non-repudiation. In order to provide a secure network, security professionals must secure the data, the network assets (e.g. devices) and the communication transactions across the network at all times. The alterations to the network architecture introduced by SDN along with 5G or other technologies must be assessed to ensure that network security is sustained. One of the network features of 5G technologies is heterogenous access, which only allow use of different access technologies such as Wi-Fi or LTE, but also support multi-network environment. That means that the access network architecture of different networks are different, so security designers of 5G technology must ensure that they are building the suitable security architecture for different access technologies.

Though SDNs provide us with the ability to easily program the network and to allow for the creation of dynamic flow policies in the network. It is, in fact, this advantage that may also lead to some potential security vulnerabilities. In [3] Kreutz et al. present a high-level analysis of the overall security of SDN. They conclude that due to the nature of the centralized controller and the programmability of the network, new threats are introduced requiring new responses. They propose a number of techniques in order to address the various threats, including replication, diversity and secure components [4]. The results of these analyses indicate that the control and data layers in SDN are still clear targets of attack.

The QoS provisioning in the advanced SDN-enabled 5G networks are more complex and poses a real problem that need to be addressed [1]. QoS automation should be supported at every wired and wireless technology that may share the same the network slice. Although SDN allows creating different network slices in the same network infrastructure to provide a strict QoS as well as performance and isolation required by across applications without interfering with traffics in other slices, however, SDN does not provide the ways for automating QoS provisioning per-application/per-service [1].

A DDoS attack refers to an attack that attempt to make a machine or network resource unavailable to its intended users. In the case of SDN, the network devices require access to the control plane to receive traffic management instructions and traffic across the network requires access to the network device flow tables to dictate traffic management policies. The data-control plane interface and the network device flow table are therefore points of vulnerability to DoS attack. Most of the current research done in SDN security focused more on the OpenFlow protocol, but the vulnerabilities that exist in OpenFlow are likely to be generalizable to any SDN system that uses a centralized controller. As per the study done in the research paper [9-11], the most common vulnerability that is noted is the communication bottleneck that is between the data-plane and the controller in an OpenFlow network.

a. Risk at Southbound API's:

Due to the lack of intelligence at the southbound APIs, they are susceptible to attack via false and forged flow table entries. The attacker may send false data stream with slightly different header information to overflow the flow table, as a result the legitimate flows cannot be updated on time. The security of the whole network could be compromised by unsecure implementation of the southbound protocols.

Suggested Solutions - The problem can be avoided by using TLS for *encryption* which can potentially avoid eavesdropping and spoofing of northbound and southbound communication, *message integrity* ensuring that the message is not altered, *authentication* by validating one or both partners to exchange using public-key certificates. The security function provided by TLS is transparent to the application and also to TCP, thus neither TCP nor application needs to be modified to invoke the security features of TLS.

b. Risk due to End Terminals/Devices:

End terminals may possess various threats including misuse or downloading of application, trojans or viruses etc. These mobile devices should also the area of focus, as any vulnerable devices may lead to vulnerability in the entire infrastructure. The terminals usually lack an effective security tools such as intrusion detection system, antivirus software, endpoint firewalls, spam blocking and so on. These end terminals/devices possess huge security risk, if not properly secured.

Suggested Solution -Make end device secure by default. When the control is unable to meet the security requirements, it should take actions such as deny by default, etc., Different security level must be implemented in order to meet the security requirement. All the end devices must have required security capabilities in place, the security application used within the network must push rules to all network devices. The devices must be check for required security compliance before giving access to them.

c. Risk at Communication layer

The protocols used in communications between base stations and controller, controller and application services are also vulnerable to attacks due to lack of the underlying IP layer security and authentication. Some of the attacks that could be possible at this layer are SYN DoS and TCP reset attack [7].

Suggested Solution: The communication channel between the controller and data plane must use IP-Sec tunneling to secure the communication between them. Intrusion Detection Mechanism should be implemented to detect the inappropriate or incorrect behavior of protocols used in this layer. Researcher in [8] also proposed a solution by using HIP and IPSec tunneling to provide secure channel between the controller and data plane layer.

d. Risk at Application layer

The 5G network support wide variety of mobile devices that might host vulnerable applications which can also be the source of attack. Hence, the application layer hosting various

applications might be vulnerable, as it can cause fault information flow to the controller or inject deceptive rules into the network. A successful attack at this risk layer could gain control of the networking infrastructure. To provide security at this layer, we must focus on preventing unauthorized applications and users from exploiting the controller.

Suggested Solution: The application layer must host application management and strong authentication mechanism. It must also ensure periodic debugging and testing of all the applications for correctness and reliability. Proper constraint must be defined for APPs, so unauthorized access by these APP can be easily detected and proper actions can be taken on time.

e. Risk at Controller layer

SDN controller when implemented in 5G provides management and router selection for all radio access network (RAN) to core network connection. But it also provides single point of failure, and if it is compromised the whole network can be under the controller of the attackers. SDN-controller is the high-value target that needs a high level of protection. The controller can also be prone to DDoS attack, if the controller is hijacked, the attacker can take over the whole network, flows and policies. Hence, SDN controller must have strong security policy so as to avoid it from any vulnerability.

Suggested Solutions: Strong security policies must be implemented to avoid DDoS attack on the controller. It is also advisable to use high availability functionality in the controller to guard against DoS attacks. We can also employ a detection system such as IDS/IPS to help identify any abnormal flows within the controller. Unauthorized access to SDN controller must be prevented and logging as well as trails must be used.

Table 1 summarizes some of the security challenges at each level that still remain possible sources of attack and proposed solutions. Research still needed to be carried out to overcome these challenges and make it stronger. The table focuses on major area of focus that need more attention implementing SDN for 5G network.

Table 1. Security challeneges and proposed solutions

Security Challenges at various levels	Problem	Solutions
At Southbound communication	There is no encryption of the traffic between the controller and switches which may leads to eavesdropping.	The problem can be avoided by using TLS for encryption which can potentially avoid eavesdropping and spoofing of northbound and southbound communication.
At the northbound communication	Due to the lack appropriate authorization at this level may potentially leads inappropriate or malicious access on the applications.	Strong mutual authentication must be implemented at this level, to validate the identity of each component.
At Application components	If the application is not verified to be from the trusted source, they might create major vulnerabilities and consequently may compromise the whole network.	Proper testing and debugging of the applications should be done to test the correctness and reliability of all the applications. Strong authentication mechanism must be enforced.
At controller Level	The controller can be prone to DDoS attack. If the controller is hijacked, the attacker can take over the whole network, flows and policies.	Implement strong security policies as well as high availability functionality to avoid DDoS attack. Backup controller must be implemented to avoid single point of failure. So, if in case the first one is compromised or unavailable, we can switch to another one without disrupting any services. Implement detection system to identify abnormal flows. Prevent unauthorized access to the SDN controller
End terminals/devices	End terminals may possess various threats including misuse or downloading of application, trojans or viruses etc.	Use strong security tools at the end terminals such as mobile devices. For example, "Micro Focus "it provides end to end mobile app security testing across multiple mobile devices, platforms, networks, servers etc. Fortify is a tool by Micro Focus which secures mobile app before getting installed on a mobile device. Additionally, all the data from mobile devices must be encrypted using strong security algorithms [12]. Mutual authentication mechanism should be used. All devices must have security capabilities.

6. Muthual Authentication between the Controller and Base Station

If the controller is implemented in the edge network connecting different base stations, in that case all the processing is being performed at the controller. As controller is the core of the network, it is highly important to secure the controller from any kind of attack. So, this paper also focuses on strong mutual authentication between the controller and the base stations before any exchange of messages. The authentication must be performed before every session and new keys must be used for each session between them, to avoid any kind of replay attack, man-in-the middle attack as well as controller hijacking.

Mutual authentication between controller and base station could be achieved by using AES as shown in figure 4. It is assumed that the random secret keys and cipher key is shared between the controller and the base station only. The controller also keeps a copy of the identity ID_B of the base-station. The notations can be summarized in Table 2 to describe the algorithm.

Table 2. Notations

Symbols	Description
K_1, K_2	Random secret keys shared between Controller and Base station
K	Cryptographic key shared between Controller and Base station
ID_B	Unique identification number of Base stations shared between the Controller and Base station
$E_k (K_1 + K_2)$	AES Cipher text, using K_1, K_2
$E_k (K_1 + K_2 + ID_B)$	AES Cipher text, using K_1, K_2 and ID_B
$E_k (K_1 + K_2)$	The notated $E_k (K_1 + K_2)$
$E_k (K_1, K_2, ID_B)$	The notated $E_k (K_1 + K_2 + ID_B)$

- *Step 1: (Challenging)*

In this step the controller will send $E_k (K_1, K_2)$ to the base station. The cipher key K and the random keys K_1, K_2 are shared by the Controller and the Base station only. It encrypts the shared keys K_1, K_2 with the cipher key K. Hence, $E_k (K_1, K_2)$ is a good measure to validate the authenticity of the controller.

- *Step 2: (Authentication of the controller)*

When the Base station receives $E_k (K_1, K_2)$, it generated $E^*_k (K_1, K_2)$ and verified the received $E_k (K_1, K_2)$ with $E^*_k (K_1, K_2)$. If $E_k (K_1, K_2) = E^*_k (K_1, K_2)$, Base station authenticates the controller. Now the base station generates $E_k (K_1 + K_2 + ID_B)$ and sends it to the controller. It is encrypted using AES128 cryptographic algorithm. Base station uses its identification information and sends it to the Controller.

The cipher key K and random numbers K_1, K_2 are shared only between the controller and the base station. Therefore, base station can detect an illegal Controller and discard the message. Consequently, the man-in-the-middle attack by an illegitimate controller and a passive eavesdropper can be prevented.

If the base station has successfully authenticated the Controller, Base station updates the shared secret keys K_1, K_2 by exclusive-ORs with $E_k (K_1, K_2)$.

- *Step 3: (Authentication of Base station)*

The base station forwards $E_k (K_1, K_2, ID_B)$ to the Controller. The controller decrypts $E_k (K_1, K_2, ID_B$ using cipher key K and random number and obtain ID_B. Then controller verifies whether ID_B is valid by comparing the obtained ID_B with ID^*_B.

Radom secrets K_1, K_2 and cipher key K are shared only between the controller and the base station. Therefore, controller can detect an illegal base station and discard the message. Therefore, the man-in-the-middle attack by an illegitimate base station and a passive eavesdropper can be prevented.

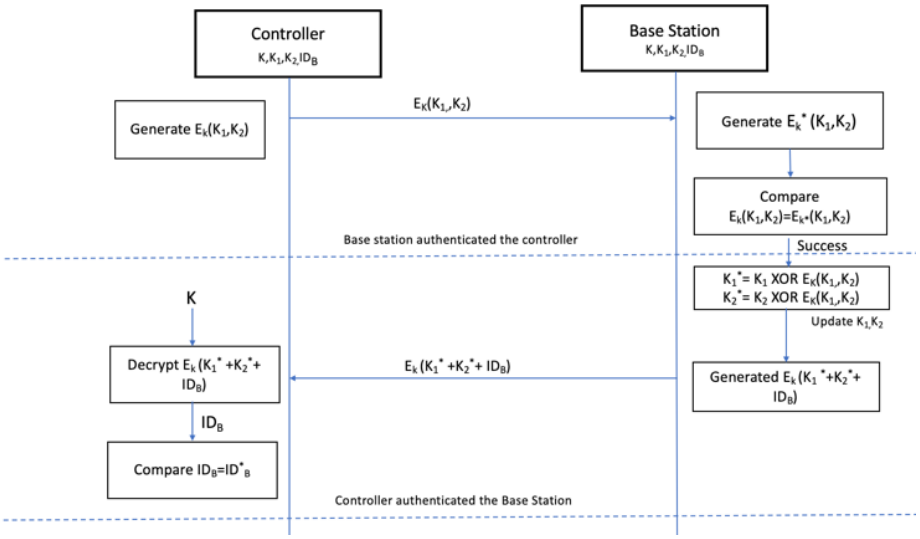

Figure 4. Mutual Authentication between the Controller and the Base Station

If the Controller has successfully authenticated the base station, controller generates E_k (K_1, K_2) with its shared random secrets K_1, K_2, and updates the shared secret keys K_1, K_2 by exclusive-ORs with E_k (K_1, K_2). Then, mutual authentication has finally succeeded.

7. Conclusions

This paper focuses mainly on security issues and challenges with the integration of SDN and 5G. Although some advances are being made by combining SDN and 5G, there are many challenging problems that need to be addresses with the integration of heterogenous technologies. Security is one of the issues that needs the significant research efforts. As these technologies are still new, many challenges and security issues still need to be solved. This paper highlights the major area that needs more attention during the implementation of SDN and 5G. It also discusses some of the problems that that exist at various levels and suggest proposed solutions for them.

REFERENCES

[1] Chen, M., Qian, Y., Mao, S., Tang, W., & Yang, X. (2016). Software-defined mobile networks security. *Mobile Networks and Applications*, *21*(5), 729-743.

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

[3] D. Kreutz, F. Ramos, and P. Verissimo, “Towards secure and dependable software-defined networks,” in Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013, pp. 55–60.

[4] Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2013, November). SDN security: A survey. In *Future Networks and Services (SDN4FNS), 2013 IEEE SDN For* (pp. 1-7). IEEE.

[5] Gupta, A., & Jha, R. K. (2015). A survey of 5G network: Architecture and emerging technologies. IEEE access, 3, 1206-1232.

[6] X. Jin, L. E. Li, L. Vanbever and J. Rexford, "SoftCell: scalable and flexible cellular core network architecture.," in CoNEXT, 2013.

[7] Principles and practices for securing software-defined networks, 2015. www.opennetworking.org.

[8] Liyanage M, Ahmad I, Ylianttila M, Santos JL, Kantola R, Perez OL, Itzazelaia MU, de Oca EM, Valtierra A, Jimenez C (2015) Security for future software defined mobile networks. In: 9th International Conference on Next Generation Mobile Applications.

[9] D. Kreutz, F. M. Ramos, and P. Verissimo. Towards secure and dependable software-defined networks. Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking - HotSDN ’13, page 55, 2013.

[10] A. Curtis and J. Mogul. DevoFlow: scaling flow management for high-performance networks. ACM SIGCOMM, 2011.

[11] A. Dixit, F. Hao, S. Mukherjee, T. Lakshman, and R. Kompella. Towards an elastic distributed SDN controller. Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking - HotSDN ’13, page 7, 2013.

[12] 10 Best Mobile APP Security Testing Tools in 2019. (2018, December 25). Retrieved from https://www.softwaretestinghelp.com/mobile-app-security-testing-tools/.