# Securing 5G Het Nets in SDN Using Authentication

**Monica Murlidhar Jagtap, S. Renuka Devi**

***Abstract:*** ***Fifth generation (5G) networks are highly heterogeneous with security being prime concern. 5G is based on Wireless Network Virtualization (WNV). A software-defined network (SDN) is used to realize WNV. SDN typically is capable of solving the requirement of a large number of devices in ultra-dense 5G architecture. However, SDN is divided into three planes, namely, application, control and data plane which are vulnerable to attacks. Programming of SDN takes place at control plane. Hence, attack at the control plane becomes single point of failure. This makes it mandatory to provide authentication at the time of bandwidth allocation to prevent spoofing type of attacks. Radio Frequency (RF) channel characteristics vary in accordance with practical conditions in random manner. This can be considered as advantageous while establishing authentication procedures. The same can be used for preventing the probability of prediction for spoofing. The paper proposes a novel approach for authenticating user equipment (UE) with strategy of full and fast authentication procedures which is based on context information (CI). This in turn is Cyclic Redundancy Check (CRC) authenticated to provide multilevel security. Mininet emulation tool is used for SDN emulation and the performance is evaluated. The results show improvements in authentication along with negligible additional latency during communication.***

***Index Terms: 5G Networks, Wireless Network Virtualization, Software-defined networks, channel characteristics, Context information, CRC based authentication, latency.***

## I. INTRODUCTION

The new era of wireless communication is emerging 5G technology [1]. Users can be connected to several wireless access technologies simultaneously due to realization of ubiquitous computing. Key features of 5G include support for Virtual Private Networks (VPNs), Wireless World Wide Web (WWWW) support, and use of flat IP. Use of flat IP enables identification of devices using symbolic names which allows 5G to be acceptable for all kinds of technologies. The numbers of elements in the data path are reduced due to the use of flat IP. This results in low capital expense (CapEx) and operational expense (OpEx). 5Gs major advantage is high data rates of up to 10Gbps, which is 100 times faster than the 4G LTE. In addition, low network latency of below 1 millisecond which contrasts latency of 30-70 ms of 4G, makes 5G, way better than its older technology. In addition to these advantages, high system capacity, energy saving massive device support and cost reduction have proposed 5G as the need of the hour.The service capabilities [2] of 5G need to satisfy all these requirements compared to its competitive technologies. 5G is characterized based on eight key features as, 1-10Gbps connections, 99.999% availability, number of connected devices 10-100x, latency of 1millisecond, 100% coverage, network energy usage reduced by 90%, bandwidth per unit area 1000x and battery life of 10 years for low power devices[3]. All these benefits come with the threat that 5G will introduce new challenges in terms of security as well as privacy protection [4]. Despite these challenges the wide area of applications that 5G will support include new use cases which include vehicle-to-vehicle and vehicle-to-infrastructure communications, smart cities, industrial automation, smart homes, health services and so many more[5]. Also, support for new industry applications along with traditional voice and data communication and a broad set of devices and applications to connect society at large [6].Support for IoT [7][8] and critical services prove that 5G wireless services will enhance mobile broadband communication. These wide ranges of applications supported by 5G make it the most promising technology to satisfy the demands of today's market.

Future internet considers, wireless network virtualization (WNV) as the most promising technology to meet its demands. Internet research test beds are using WNV actively. For the ultra-dense 5G networks with tremendous wireless traffic and service requirements, the infrastructure has to be separated from the services it offers. Network utilization can be maximized by allowing differentiated services to reside on the same underlying infrastructure. New products and technologies can be supported along with legacy products by WNV by isolating part of the network. The emerging heterogeneous wireless networks demand for a stronger network management mechanism. To achieve this, we require wireless network virtualization [9].

In SDN network architecture, the network control is directly programmable [11] and is decoupled from forwarding. By separation of the control logic form its physical switches and routers, the network operators can write high-level control programs. This allows them to specify the behavior of the entire network. In contrast, the network operator of the conventional network would have to code the functionality of low-level devices. SDN provides a controller which allows the network administrator to centrally control the network programmatically, without physical access to networks switches. Hardware is not physically coupled with data forwarding plane in SDN. This is possible as logical control plane is created by SDN. Control plane and data plane are implemented separately. Runtime base environment tasks and the control plane

**Revised Manuscript Received on June 05, 2019**

**Monica Murlidhar Jagtap**, School of computing science and engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India.
**S. Renuka Devi**, School of computing science and engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India.

tasks are run using a differentiated platform. Here we introduce OpenFlow which is a standard communications interface between forwarding layers and controls of the SDN architecture [12]. Open Networking Foundation (ONF) manages this standard. Direct access to and manipulation of forwarding plane off the network devices, like switches and routers is allowed by the OpenFlow. The software running on multiple routers can determine the path of network packets through the network of switches in OpenFlow. OpenFlow standard are likely to be promoted by a number of vendors to support their routers and switches.

Several factors need to be considered while focusing on the security aspects of 5G technology. New 5G protocols can be defined by considering the attack resistance. Username/password technique for authentication should be phased out. There is a need for measurable security assurance and compliance to address new threats such as verifying presence, correctness and sufficiency of the security functions.

Currently, providing authentication to the physical layer attributes is considered most secure in SDN. The reliable approach development may involve, verifying the multiple parameters of physical layer.

Knowing that authentication using conventional cryptographic techniques applied at upper layers is no more safe for spoofing attacks. Thus, we need to plan for authentication techniques applicable at the physical layer. In this paper we propose a novel approach for authentication at physical layer. In addition to it, instead of depending on a single authentication approach, we couple two authentication techniques resulting in a hybrid security approach. The first authentication provided using context information (CI) that in turn being CRC authenticated.

We also evaluate the time taken for processing the authentication method by simulating the required analytical model using python and scipy based signal processing toolbox which shows optimum results.

This paper includes following sections. Section II focuses on related work. Developments on SDN, its requirements, current threats to SDN, solutions to it and its advantages are highlighted in section III. The proposed hybrid security model is shown in section IV. Section V consists of performance evaluation which includes introduction to Mininet, its scripting and results of our work. Section VI concludes the paper.

## II. RELATED WORK

Research related to WNV, SDN and authentication is a vast domain. Providing authentication for 5G is need of the hour. In this context we focus on available literature. Some of the key areas are addressed here.

E. Kitindi et al [10], focus on how WNV has drawn attention of researchers as the need of future internet. The paper surveys latest developments in the SDN technology. It proposes a general architecture for the WNV based on SDN. It also shows challenges and research issues for future network communication. The paper forms the platform of understanding the WNV.

D. Fang, Y. Qian and Rose Hu [13] the authors give a survey on security challenges for 5G networks. 5G network review is given in the paper along with requirements and motivation for securing the 5G technology. Based on the survey, the authors propose new security architecture for 5G wireless networks, which includes authentication and key agreement process along with handover scenarios and signaling mechanism. As authentication procedure suggested by authors is required to be done at each handover, increment in latency is main disadvantage.

N. Xie and S. Zhang [14], authors here present physical layer authentication in contrast to conventional authentication provided using cryptographic tools at the upper layers. The method combinesblind known interference cancellation (BKIC) technique with the differential processing (DP) to implement authentication. The advantage of authentication at physical layer provides enhanced security as it poses uncertainty to the attackers. Efficiency and compatibility is enhanced by avoiding operations at the upper layers. This is of prime importance for heterogeneous environments like 5G wireless systems.

X. Duan and X. Wang[16], have given idea of authentication using weighted secure context information. The approach given by author's shows sufficient level of security to avoid spoofing attacks in 5G networks. The weighted approach is used to for assigning priority structure of authentication requirement based on which fast or full authentication is decided. The experimentation results show that the additional latency due to this approach is at optimum level. The only drawback is implementation complexity involved in calculation process. Also additional packet overhead evaluation shows additional network overhead.

E. Dubrova, M. Näslund and G. Selander[17], have given CRC based approach along with random polynomial generator for authentication process along with error control. The experimentation scenario for network model is not considered and analytical approach is considered for evaluation of the algorithm.

L. Zulu et al [20],have proposed how Mininet is one of the best options for implementing SDN. Mininet is a network emulator. It creates a virtual network similar to the real network which helps in understanding how SDN actually works.

F. Ketiet al [23], have proposed key characteristics of Mininet which includes flexibility, applicability, and interactivity, scalability, realistic and shareable. Software defined network prototype can be created by the programmers in a simple manner that can be customized, shared with and run on a hardware.

By going through all the above papers we can conclude that authentication is the need for securing the emerging 5G technology. Knowing that authentication using conventional cryptographic techniques applied at upper layers is no more safe for spoofing attacks. Thus, we need to plan for authentication techniques applicable at the physical layer. In this paper we propose a novel approach for authentication at physical layer. In addition to it, instead of depending on a single authentication approach, we couple two authentication techniques resulting in a hybrid security approach. The first authentication provided using context information that in turn being CRC authenticated.

## III. SDN, THREATS TO SDN AND AVAILABLE SOLUTIONS

Open Data Center Alliance (ODCA) lists the requirements of modern networking under seven points as: Adaptability, Automation, Mobility, Maintainability, Integrated security, Model Management and On-demand scaling. SDN covers all these requirements along with openness and flexibility in contrast to proprietary systems.In SDN approach the control plane and data plane are on separate devices. The switching function is split between these two planes. Here forwarding of packets is the responsibility of the data plane. Physical switches and virtual switches constitute the data plane. Control plane in turn is responsible for meeting the QoS and QoE requirements by setting priority and routing policy parameters, designing routes and to cope with the shifting traffic patterns. Open interfaces are included to present a uniform interface regardless of internal implementations and enabling the SDN controllers communicate with the networking applications. Implementation of the SDN controllers can be done on a server or a virtual server.

A list of attacks on SDN are summarized in [15] as: Eavesdropping, Distributed Denial of Service (DDoS), Password-related attacks, Identity spoofing, Sniffer attack, Applications attack, Man in the Middle (MITM) attack, Denial of Service (DOS), Sensitive Data Protection, Security into software.

Figure 1 shows SDN architecture that is exposed to security attacks at any of the three layers as well as during communication between the layers. According to the figure 1, hardware or the software attack can occur at any layer of SDN. The protocol attacks occur in between the planes during communication.

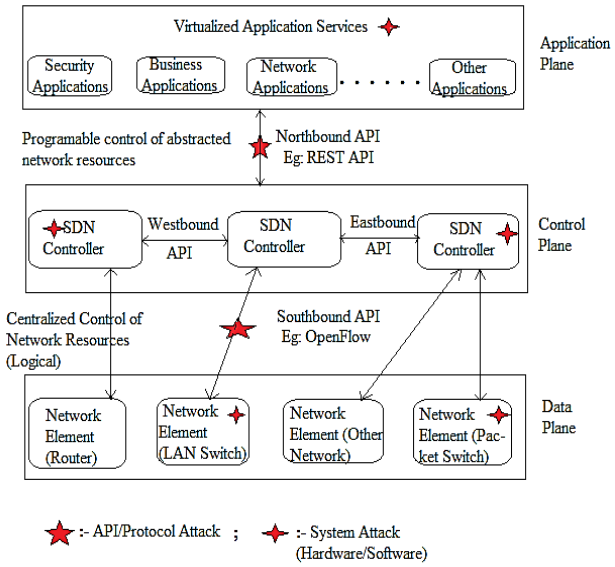


**Figure 1: SDN security attack diagram**

Possible solutions for ensuring network security by using SDN system are addressed in [15].

Figure 2 shows the block diagram for the proposed security approach. This authentication is applied at each plane of the SDN.

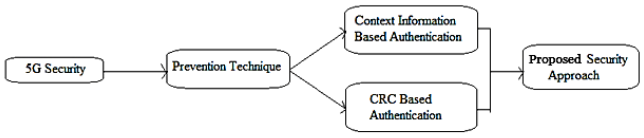


**Figure2: Proposed Security Approach**

Current drawback in providing security is, the authentication techniques used in isolation. This results in poor primary level of defense for 5G systems. Hence we propose a new security approach which uses CI and CRC techniques to come up with a robust protection for 5G networks with minimum network overhead. The detailed explanation for implementation of each technique is given in section IV.

## IV. PROPOSED SECURITY MODEL

The proposed work consists of a novel approach for authentication in SDN implemented in two modules.

The first module for authentication is using context information (CI) of user equipment (UE)[16]. In this paper we make use of the fact that context information involves the effect of variety of parameter. These parameters can be the location of user equipment, the channel impulse response, fading effect of channel and noise characteristics of the channel. Specifically, with respect to location and channel allocation, channel impulse response can be considered as key parameter for estimating and cross verifying the UE. These parameters are unpredictable as they vary dynamically. This makes attacking the UE difficult resulting in better security. The second module involves the CRC based approach [17].

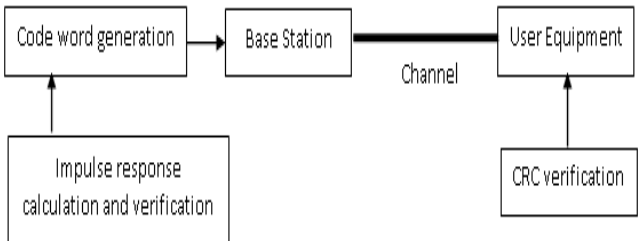


**Figure 3: Conceptual block diagram of proposed work**

### *A. CI based UE authentication*

The channel based transmitter to receiver communication depends on variety of parameters. The receiver and transmitter locations are important to estimate the effect of channel on each bit of communication. The effect of channel depends on parameters like fading, noise addition, channel impulse response and interference in the communication frequency. The authentication strategy can be developed based on these parameters verification strategy. When transmitter to receiver communication is to be established, authentication is required to achieve security and privacy. This process also should not be overhead to the network. The bandwidth utilization and network resource utilization performance should not degrade. This can be done using fast authentication strategy as detailed further.

The network parameters as context information in terms of location, channel impulse response, effect of noise and fading effects of channel are considered as actual effects

for particular receiver. The UE is authenticated using these parameters. The effect on channel impulse response along with location is packed into one packet by calculating at one of the station and sent to other station for verification purpose. The verification can be done using comparison based process in which pre calculated parameters and actual received parameters are compared. As these channel effects are not steady state responses and varies with respect to practical conditions, the comparison process thresholds may require to be set to particular values with sufficient tolerances.

Let X be the vector of contextual information, which contains channel impulse response vectors such as, $x_1$, $x_2$, …,$x_n$.

$$X = \begin{matrix} x_{11} & \dots & x_{1n} \\ x_{21} & \dots & x_{2n} \\ x_{31} & \dots & x_{3n} \end{matrix} \quad \dots(1)$$

This impulse response depends on UE location, fading effect and noise effect. These predefined parameters can be considered for calculating the channel impulse response while authentication process for the first time. In [18], localization technique is given which is based on channel impulse response for indoor applications. The effect on channel due to AWGN noise is also considered while calculating the location of the equipment. We estimate channel impulse response using location. The channel impulse response is used to estimate the received data from sent data in normal scenarios as shown in [19]. In our approach we use sent and received data to estimate channel impulse response.

In our approach, we estimate the channel impulse response for time and distance varying multipath fading channel. Let X'(t,r) be the channel impulse response at practical. Where t indicates time varying signal due to motion of the equipment and r indicates the multipath delays. Let x(t) and y(t) be the fixed coordinates functions to estimate the channel impulse response stored in the database at each equipment t. The X' is calculated at UE and sent along with the location through packet to base station for authentication.

When authentication process is required, base station equipment can calculate the impulse response using x(t) and y(t) from the database and location sent by the UE. The vector X obtained as in equation (1)is then compared with received vector X'.

Where,

$$X' = \begin{matrix} x'_{11} & \dots & x'_{1n} \\ x'_{21} & \dots & x'_{2n} \\ x'_{31} & \dots & x'_{3n} \end{matrix}$$

Let, ΔX be the difference between the calculated and received vectors given as,

$$\Delta X = X - X' \quad \dots(2)$$

In case of normal environmental conditions, the channel impulse response varies randomly up to certain limit compared to calculated values using sent and received data. Let Th be the threshold allowed to compensate tolerance of the difference between calculated impulse response and received impulse response in normal environmental conditions. By comparing ΔX with Th two conditions are possible,

*If* ΔX <Th*then* UE is authenticated, *else* not authenticated.

### *B. CRC based UE authentication*

The Cyclic Redundancy Check has been used to address security issues by using message authentication by 3G or LTE based networks so far. The Linear Feedback Shift Register with g(x) as a connection polynomial has been implemented efficiently for CRC encoding and decoding. Detection of random errors is done using traditional CRCs, with one limitation that it does not provide strong mechanism for malicious advisories. We can enhance the secure and error free communication by using cryptographic hash functions with speedy computing methods for generator polynomial calculations.

In contrast to the process of CRC based authentication as shown in [17], we first fix the polynomial multiplier in generator polynomial, to bring the randomness, by using channel impulse response vector as shown in equation (3). The message polynomial is multiplied by $x^n$and divided by generator polynomial g(x).

$$g(x) = x^3+x+1 \quad \dots(3)$$

By considering polynomial in (3) code word is calculated as,

$$r(x) = M(x).\ x^n \bmod g(x)$$
$$c(x) = M(x) + r(x) \quad \dots (4)$$

Where, r(x) is remainder, M(x) is message, and c(x) is codeword.

### *C. Proposed approach of authenticating UE*

Selecting fixed generator polynomial, leads to easy identification of the codewords for the attackers. Hence we keep the generator polynomial as random as possible to make it difficult to guess for the attacker. Hence g(x) can be given as,

$$g(x) = (x^3+x+1) \cdot X' \quad \dots (5)$$

Where, X' is impulse response vector used for generator polynomial.

The algorithm of proposed system is as detailed further.

***Algorithm:***

***Base Station Side:***

1. *Receive the channel impulse response X*
2. *Calculate the channel impulse response X' locally using location of user equipment*
3. *Estimate the difference* ΔX= X-X'
4. *If ΔX <=Th*
   *Authenticate*
   *Else*
   *Do not authenticate*
5. *Generate code word, C = M(x) + r(x)*
   *Where, r(x) = M(x). $x^n$ mod g(x)*
   *Where, g(x) = g(x)= $(x^3+x+1) \cdot X$*
6. *Send the code word*

***User Equipment Side:***

1. *Send location information along with Channel Impulse Response Information (X)*


Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

2. *Receive the code word for CRC*
3. *Extract code word to message word using X*
4. *Estimate CRC and verify to that received.*
5. *If CRC matches, authenticate else, drop the message.*

For the first time, calculation of impulse response process is required. For upcoming continuous authentications, simply pre calculated impulse response can be used and this can be stored in the database for the purpose, temporarily. Hence, as there is no requirement of re calculation of impulse response, further authentication delays are reduced thereby less effects on latency of communication. Here new condition is required to be handled that, when first authenticated UE loses its actual channel characteristics due to movement and other practical scenarios such as noise, the authentication may get lost and communication will be stopped. In this case again recalculation of impulse response may solve the issue which is full authentication process.

Figure 4 shows the process flow in base station and user equipment for communication along with authentication using proposed algorithm.

## V. PERFORMANCE EVALUATION

The proposed System is implemented in Mininet open flow emulator for experimentation. The architecture used for experimentation is kept simple as possible to evaluate the proposed algorithms. The proposed system architecture is shown in the figure 5. The architecture used in the experimentation consist of the main blocks as,

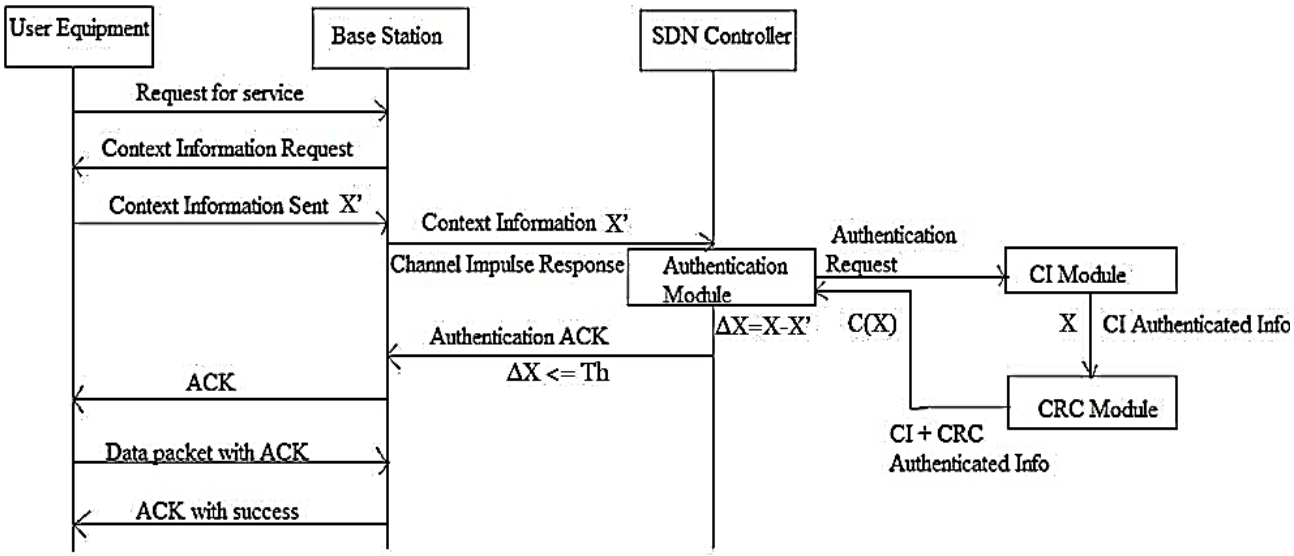


**Figure 4: Process flow for authentication using proposed algorithm**

### A. SDN Controller

The Openflow protocol based interfaces are provided by SDN controller which provides service of network resource management in logically centralized and physically distributed manner. The SDN is responsible for estimating the resource capabilities with respect to their allocations to respective end nodes. The context information needed for authentication will be estimated by SDN controller for each channel allocated to the user equipment. In this case, we have set total number of user equipment to one. The channel impulse response as a user equipment identity is evaluated using script attached with the SDN controller block along with verification script.

### B. Infrastructure Manager

It is in charge of the infrastructure layer, by monitoring the processing and storage status of servers. The infrastructure manager is used here to record the network operations and interfaces allocation in log file.

The specific interfaces used in this architecture are detailed as,

Interface $I_1$: The interface between Base station and SDN controller

Interface $I_2$: The interface between base station and Infrastructure Manager

Interface $I_3$: The interface between SDN Controller and Infrastructure manager

Interface $I_4$: The interface between User Equipment and Base Station (channel)

Mininet creates a virtual network similar to real network[20]. It provides a platform to test how SDN works on small and large networks. Distributed SDN has evolved as a need for fault tolerance and scalable operating systems and applications [20].An emulator which can produce reliable results to incorporate such networks[21] is required.Applications tested on SDN can easily be deployed on a real network [22]. Key characteristics of Mininet which includes flexibility, applicability, and interactivity, scalability, realistic and shareable[23]. Advantages of Mininet include support for collaborative network research, lightweight approach of OS virtualization, scalability and debugging in real-time [24][25]. Experiments conducted using Mininet [26] produced successful results.

Apart from Mininet several other simulators are available popular amongst them include Raspberry-Pi [27] and Fs-SDN [28]. These simulators however use full system virtualization, complex coding, system overheads and decreased usability. These factors make Mininet simulator of choice for SDN. All these features of Mininet made us choose it as the emulator for our work.

In our work the context based approach is

implemented using python and scipy signal processing toolbox for verifying the latency effects due to additional time of authentication process. CRC based authentication algorithm is implemented using python. This is used for estimating the performance of bit error detection and correction.

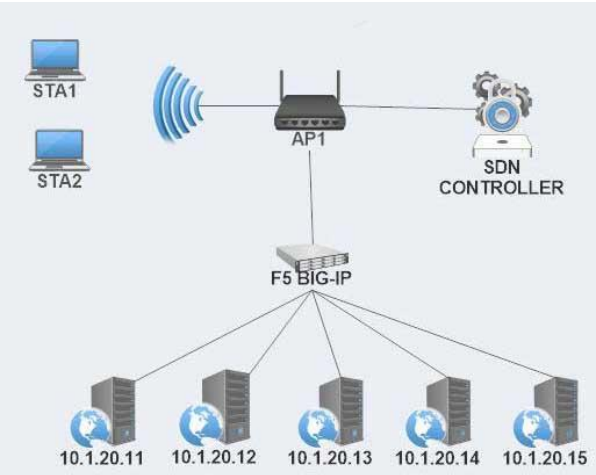


**Figure 5: Mininet Implementation**

## VI. CONCLUSION

In SDN, channel characteristics vary in accordance with allocation factors based on spectrum characteristics. The allocated channelto the UE is required to be authenticated every time UE interacts with the BS as a matter of security.This paper shows a novel approach for authentication, using context information (CI) of channel allocated to UE.In generalized scenarios, there are limitations of authentication using only CRC based approach with the fixed generator polynomial. Hence a random generator polynomial can provide solution to the challenge as indicated in [17].The combination of CI and CRC approaches along with sufficient randomness in generator polynomial in CRC by keeping less complexity in computation can provide greater security level compared to each technique alone. Due to this, the probability of prediction of generator polynomial is quiet less and depends on actual location of the UE, which also varies randomly. This increases the robustness and reliability of our authentication scheme.The results show improved security due to double authentication along with negligible levels of additional latency in the network. Low latency showspractical feasibility of implementation.

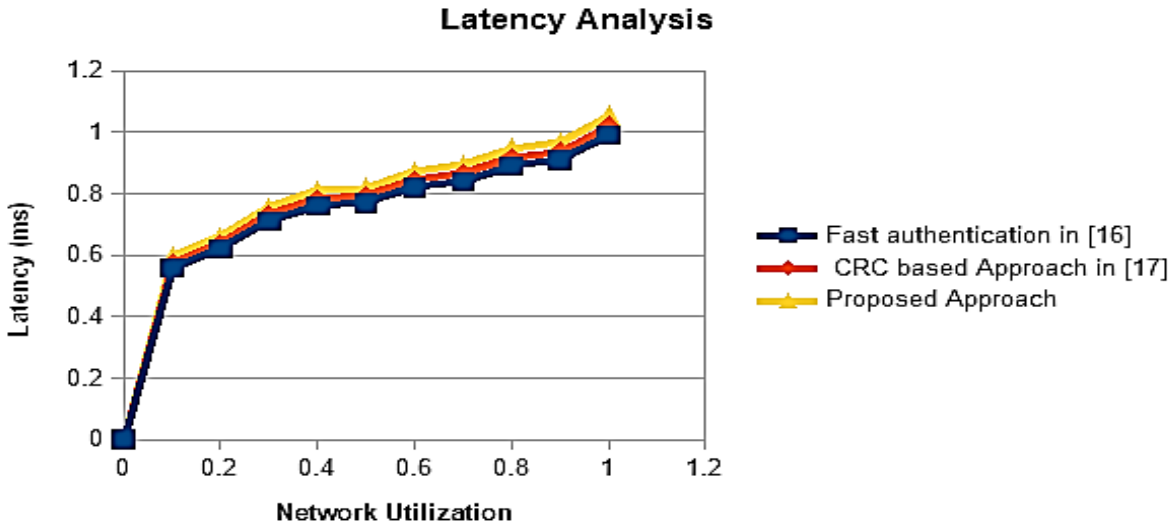


**Figure 6: Comparative analysis of proposed method with the method in [16, 17]**

This also achieves authentication and hence multipurpose operation of CRC. Also, then combination of above approaches is implemented in Mininet to evaluate the latency performance. The comparative analysis helps to understand that there is very negligible latency once full authentication is done. The proposed approach consist of two step security for authentication verification and hence more secure than single type [16]. Also, effect of additional computation has less impact on latency as shown in the graph of figure 6.

The latency analysis shows that there is slight increase in delay for proposed approach compared to CRC based approach and approach in [16]. As there is very little impact on delay and which is up to acceptable level, the proposed system shows implementation feasibility in practical applications. This slight increase in delay is acceptable when compared to improved security due to robust and random CI factors extracted from UE. This in turn CRC authenticated by considering the random polynomial instead of a fixed polynomial.

## REFERENCES

1. N. Panwar, S. Sharma and A. K. Singh, “A Suvery on 5G: The Next Generation of Mobile Communication”, Physical Communication, vol. 18, no. 2, pp. 64-84, 2016.
2. “5G Vision”, 5G PPP, February, 2015.
3. “Understanding 5G: Perspectives on future technological advancements in mobile”, GSMA Intelligence, December, 2014.
4. “5G Security: Forward Thinking Huawei White Paper”, HUAWEI WHITE PAPER, 2015.
5. “The Road to 5G: Drivers, Applications, Requirements and Technical Development”, GSA, November, 2015.
6. “5G SECURITY”, ERICSSON WHITE PAPER, June, 2015.
7. “Leading the world to 5G”, QUALCOMM, February, 2016.
8. J. G. Andrews et al., “What Will 5G Be?”, IEEE Journal on Selected Areas in Communications, vol. 32, no. 6, pp. 1065-1082, 2014.
9. H. Wen. P. K. Tiwary, and L.-N. Tho, ”Current trends and perspectives in wireless virtualization,” in Proc. Int. Conf. Sel. Topics MoWNet,

Montreal, Canada, Aug. 2013, pp. 62-67.
10. EDVIN J. KITINDI, SHU FU, YUNJIAN JIA, (Member, IEEE), ASIF KABIR, AND YING WANG "Wireless Network Virtualization With SDN and C-RAN for 5G Networks: Requirements, Opportunities, and Challenges" Digital Object Identifier 10.1109/ACCESS.2017.2744672, IEEE 2017.
11. Open Networking Foundation, "Onf white paper: Software-defined networking: The new norm for networks," Palo Alto, CA, USA, 2012, Tech. Rep.
12. N. McKeownet al., "Openflow: Enabling innovation in campus networks," SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69-74, Apr. 2008.
13. Fang, Y. Qian and Rose Hu, "Security for 5G Mobile Wireless Networks" DOI 10.1109/ACCESS.2017.2779146, IEEE Access.
14. N. Xie and S. Zhang, "Blind Authentication at the Physical Layer under Time-Varying Fading Channels" DOI 10.1109/JSAC.2018.2824583, IEEE Journal on Selected Areas in Communications.
15. Christos Bouras, Anastasia Kollia, Andreas Papazois, "Teaching network security in mobile 5G using ONOS SDN controller".
16. XiaoyuDuan and Xianbin Wang "Fast Authentication in 5G HetNet through SDN Enabled Weighted Secure-Context-Information Transfer" IEEE ICC 2016 Communication and Information Systems Security Symposium, 2016.
17. Elena Dubrova, Mats N¨aslund, G¨oranSelander "CRC-Based Message Authentication for 5G Mobile Technology" 2015 IEEE Trustcom/BigDataSE/ISPA.
18. Yunye Jin et al, "Indoor Localization with Channel Impulse Response Based Fingerprint and Nonparametric Regression", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 9, NO. 3, MARCH 2010.
19. Impulse Response Model of a Multipath Channel – National Instruments, "Impulse Response Model of a Multipath Channel", Publish Date: Jul 19, 2018.
20. L. Zulu, K. Ogudo, P. Umenne, "Simulating Software Defined Networking Using Mininet to Optimize Host Communication in a Realistic Programmable Network", 978-1-5386-3060-0/18/$31.00 ©2018 IEEE.
21. N. Handigol, B. Heller, V. Jeyakumar, B. Lantz and N. McKeown N. "Reproducible network experiments using container-based emulation". CoNEXT'12, Nice, France, December 2012.
22. B. Lantz and B. O'Connor, "A Mininet-based virtual testbed for distributed SDN development". Monterey, CA, USA. 2010.
23. F. Keti and S. Askar, "Emulation of Software Networks Using Mininet in Different Simulation Environments" 6th International Conference on Intelligent System, Modelling and Simulation, 2015.
24. B. Lantz, B. Heller and N. McKeown N. "A network in a laptop: rapid prototyping for software-defined Networks." Hotnets '10, Monterey, CA, USA, October 20-12, 1010.
25. Syrivelis D, Parisis G, Trosse D. Flegkas P, Sourlas V, Korakis T, Tassiulas L. "Pursuing a software defined information-centric network". Paper presented at the European workshop on Software defined Networks in Darmstadt, Germany from 25-26 October 2012.
26. Kumar and M. Sood. "Software defined networks (S.D.N): experimentation with topologies". Indian Journal of Science and Technology, Vol 9(32). August 2016. August 2016.
27. J. Weerawardhana, N. Chandimal and ABandaranayake. "SDN testbed for undergraduate education". Proceedings of the Fourth Engineering Students', Conference at Peradeniya (ESCaPe'15), 2015.
28. H. Kim, J. Kim and Y. B, Ko, "Developing a cost effective OpenFlowtestbed for small-scale Software Defined Networking,"16th International Conference on Advanced Communication Technology, pp. 758-761, Pyeongchang, South Korea 2014.

## AUTHORS PROFILE

**Monica Murlidhar Jagtap,** received her Bachelor of engineering degree in Computer Science and Engineering from Visvesvaraya Technological University, Belgaum, India in 2010 and her Master of Technology degree in Computer Science and Engineering from Visvesvaraya Technological University, Belgaum, India in 2012. She is Ph.D. Student in School of Computing Science and Engineering in Vellore Institute of Technology, Chennai, India. She is lifetime member of ISTE and NMRS. Her current research areas include computer network and security.

**S. Renuka Devi,** received her doctorate degree in Information and Communication Engineering from Anna University, Chennai, India in the year 2015. She is currently working as an Associate Professor in the School of Computing Science and Engineering, VIT University, Chennai, India. Her area of interest includes Network Security and Cryptography.