SDN Enabled QoE and Security Framework for Multimedia Applications in 5G Networks

PRABHAKAR KRISHNAN, KURUNANDAN JAIN, PRAMOD GEORGE JOSE, and KRISHNASHREE ACHUTHAN, Center for Cyber Security Systems and Networks, Amrita Vishwa Vidyapeetham, Amritapuri, India
RAJKUMAR BUYYA, Cloud Computing and Distributed Systems (CLOUDS) Lab, School of Computing and Information Systems, The University of Melbourne, Australia

The technologies for real-time multimedia transmission and immersive 3D gaming applications are rapidly emerging, posing challenges in terms of performance, security, authentication, data privacy, and encoding. The communication channel for these multimedia applications must be secure and reliable from network attack vectors and data-contents must employ strong encryption to preserve privacy and confidentiality. Towards delivering secure multimedia application environment for 5G networks, we propose an SDN/NFV (Software-Defined-Networking/Network-Function-Virtualization) framework called *STREK*, which attempts to deliver highly adaptable *Quality-of-Experience* (QoE), Security, and Authentication functions for multi-domain Cloud to Edge networks. The *STREK* architecture consists of a holistic SDNFV dataplane, NFV service-chaining and network slicing, a lightweight adaptable hybrid cipher scheme called *TREK,* and an open RESTful API for applications to deploy custom policies at runtime for multimedia services. For multi-domain/small-cell deployments, the key-generation scheme is dynamic at flow/session-level, and the handover authentication scheme uses a novel method to exchange security credentials with the Access Points (APs) of neighborhood cells. This scheme is designed to improve authentication function during handover with low overhead, delivering the 5G ultra-low latency requirements. We present the experiments with both software and hardware-based implementations and compare our solution with popular lightweight cryptographic solutions, standard open source software, and SDN-based research proposals for 5G multimedia. In the microbenchmarks, *STREK* achieves smaller hardware, low overhead, low computation, higher attack resistance, and offers better network performance for multimedia streaming applications. In real-time multimedia use-cases, *STREK* shows greater level of quality distortion for multimedia contents with minimal encryption bitrate overhead to deliver data confidentiality, immunity to common cryptanalysis, and significant resistance to communication channel attacks, in the context of low-latency 5G networks.

CCS Concepts: • **Security and privacy → Security protocols**; *Symmetric cryptography and hash functions*; • **Networks → Network security**; **Network architectures**;

Additional Key Words and Phrases: SDN, NFV, 5th Generation network (5G), Multi-Access Edge Computing (MEC), lightweight cryptography, QoE, network slicing, multimedia communication, network security

Author's addresses: P. Krishnan (corresponding author), K. Jain, P. G. Jose, and K. Achuthan, Center for Cyber Security Systems and Networks, Amrita Vishwa Vidyapeetham, Clappana PO, Kollam District, Kerala - 690525, India; emails: {kprabhakar, kurunandanj}@am.amrita.edu, pramodgeorgejose@am.students.amrita.edu, krishna@amrita.edu; R. Buyya, Cloud Computing and Distributed Systems (CLOUDS) Laboratory, School of Computing and Information Systems, The University of Melbourne, Doug McDonell Building, Parkville Campus Melbourne, VIC 3010, Australia; email: rbuyya@unimelb.edu.au.

1551-6857/2021/04-ART39 $15.00
https://doi.org/10.1145/3377390

ACM Reference format:
Prabhakar Krishnan, Kurunandan Jain, Pramod george Jose, Krishnashree Achuthan, and Rajkumar Buyya. 2021. SDN Enabled QoE and Security Framework for Multimedia Applications in 5G Networks. *ACM Trans. Multimedia Comput. Commun. Appl.* 17, 2, Article 39 (April 2021), 29 pages.
https://doi.org/10.1145/3377390

1 INTRODUCTION

In recent years, multimedia applications and online streaming traffic have been rapidly developing across both wired and wireless cellular networks. A plethora of rich multimedia applications is being deployed over various wireless networks such as 5G, Narrowband IoT [1]. The researchers forecast [2] a massive explosion of multimedia content consuming more than 90% network bandwidth in world-wide network infrastructures. The multimedia streaming services may represent up to 50% of global network traffic. The emerging paradigms in cellular and wireless networking technologies, such as 5G, MEC, SDN, NFV, Software Defined-WAN (SD-WAN) and Cloud Radio Access Network (Cloud-RAN) are deployed to scale multi-folds, deliver high-speed and low latencies for mobility, and be resilient to cyberattacks. Many of the new-age digital content distribution and multimedia services (e.g., Video on Demand, Interactive 3D, 4k/8k ultra-high-definition video, immersive gaming media, e-learning, virtual and augmented reality platforms) are expected to dominate the traffic in future networking infrastructures. This will raise unprecedented demands for blazing speeds, lower latencies, availability, and seamless mobility from the infrastructure providers [4]. The emerging networks and advanced computer vision applications pose new challenges for securing multimedia applications, communication channel, and content, as they pervade rapidly over the *always-on* ubiquitous Internet. Though the multimedia interactive and content distribution applications offer high quality of experience and ease of usability, security, privacy, and confidentiality of data are major concerns lacking trustworthy solutions [5]. The modern-day Content-Delivery-Network (CDN) service providers *overlay* the rich multimedia communication protocols on less secure *underlay*, which consists of an insecure and open network or the public Internet. So, the onus is on the content sender(s) that the packets are safely transmitted, and the receiver(s) can reconstruct the original content without any interception and unauthorized access to the contents. The challenges are more so for the multimedia content in social media, as it may involve a breach of privacy and content alteration and so on. The common authentication techniques are watermarking, encryption, streaming, and hashing. The present public internet infrastructure carries heavily volatile network traffic, which poses new challenges and new dynamically adapting mechanisms are to be put in vantage points to deliver a smooth multimedia experience to clients/applications. To this end, the new SDN architecture with a programmable control, centralized with a global topology, separate *forwarding* (Dataplane), *routing* (Control plane), and *OpenFlow* [5] protocol is promising and expected to be widely adopted in production systems as well.

There has been very active research for developing enabling technologies and networking architectures, implementations of standard protocols in the field of 5G. We need more focused investigations to be done by the applications community in terms of adapting the application deployments to the emerging network softwarization and virtualization models (SDNFV) and improve the QoE and resource utilization, security, especially in the multimedia-rich digitally interconnected smart environment. The simplified traffic management, dynamic reconfiguration of policies and control, seamless mechanisms and interface for applications to get feedback from the real network for end-to-end visibility enables to alter logic or paths, especially in the 5G infrastructures. In the highly interconnected world of smart *things*, new paradigms such as Multimedia Internet of Things (MIoT) [7] consist of a farm of video cameras, surveillance monitors, microphones,

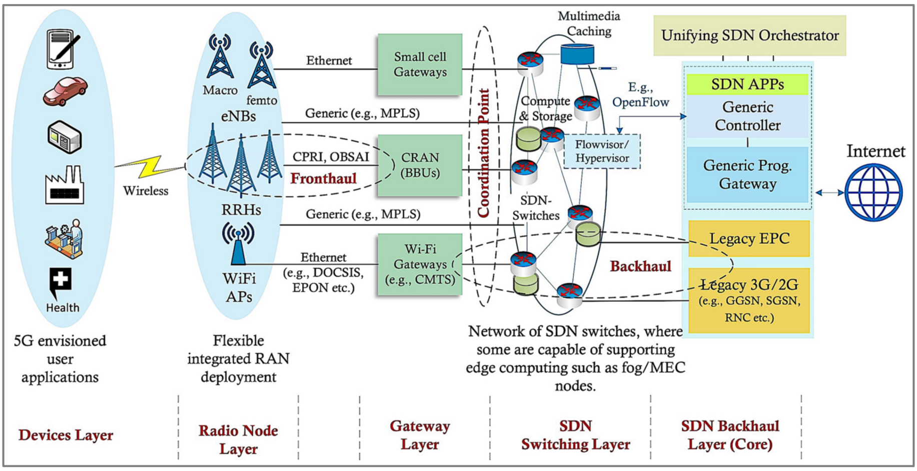


Fig. 1. SDN/NFV enabled modern network architecture [40].

and IoT sensors/actuators. The MIoT architecture can provide a plethora of services and the communication channel and data transmitted have to be secure from network attacks such as jamming, MITM, and eavesdropper attacks. The MIoT applications, multimedia devices, and networks have limited capabilities and to facilitate security and QoE services in a smart environment, only lightweight mechanisms are practical instead of traditional heavyweight approaches. The MIoT and 5G-compliant devices cannot meet the National Institute of Standards and Technology (NIST, US)-recommended security compliance requirements, and the service providers cannot deliver the guaranteed QoS/E to the end-users. To this end, the emergence of lightweight crypto algorithms has solved the major constraints to some level and still offer reasonable security. Future infrastructures for 5G, Industry4.0, Wireless Sensor Networks (WSN), Clouds are expected to be software-defined to orchestrate the traffic and to shape the dynamic requirements of the network. MEC model [8] originated from the European Telecommunications Standards Institute (ETSI) with the notion of application processing to the edge, closer to end-user devices. As this model got adopted by mobile network operators (MNOs), due to the proliferation of diverse devices IoT/smart sensors/smartphones, the advantages of this model extended beyond conventional cellular networks. Such localized processing of services will significantly reduce the latency, delay, or failures on the WAN and enhance resource utilization, customer experience, and end-to-end performance of the 5G networks. A conceptual model for integrating the SDNFV technologies into a large-scale modern network is illustrated in Figure 1. The network consists of various layers with the radio access network (RAN) as the key layer interconnecting the uplink layer (Internet) through a series of glue-layers, comprising gateway layer, the relevant SDN controlling software, switches, and a coordination layer between them. These layers delineate the RAN front-haul and backhaul. The central SDN orchestrator deployed in an edge node (with higher capability) controls the operations, security, and service requirements of the entire network. The main objective of the MNOs is to deliver services closer to customers such as IoT smart applications, streaming, Virtual Reality, and on-demand services. The MNOs employ multi-access edge infrastructure and content hosting strategies that can provide low-latency and location-based services closer to the subscribers.

The *Network slicing* is one of the key features offered by 5G technologies and brings about great improvements to network resource management and optimization. Some include: (a) logical networks with customized resource allocation perform better than *one-size-fits-all*; (b) scaling the

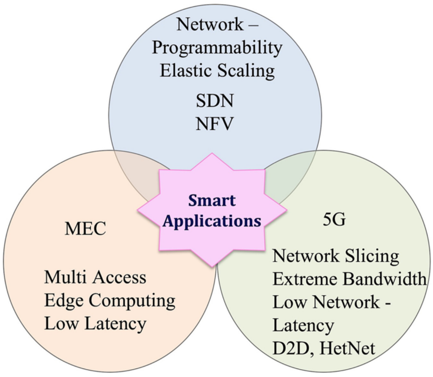


Fig. 2. Convergence of emerging paradigms.

service requirements coordinated based on usage (radio resources, switching bandwidth) and User Plane programmability; (c) isolation of the network resources among various slices increases the reliability and security of each slice; (d) to share physical infrastructure with multiple virtual disjoint networks. In a modern vehicular network architecture, considering the mobile characteristics of the connected vehicles, location-enabled smart devices, and end-User Equipment (UEs/mobiles), it is expected to deliver an optimal content acquisition and session continuity during the transition from one cell to another cell. The authentication and key management are challenging in 5G mobile networks, as there is constant mobility of subscribers and mobiles roam between small cells. So, the frequent leaving/joining of mobile users lead to busy session transition and handover protocol processing and consequently the latencies to apps.

The demands of modern applications in terms of privacy, security, and QoS/E parameters such as high bandwidth, low latency and jitter, context awareness, and mobility support are realized by utilizing emerging advanced networking paradigms such as SDN, SD-WAN, and NFVs. There are other aspects including management, control, virtualization, and integration with orchestrator provided by the MEC. (ETSI [8]). The NFV and SDN *softwarized/virtualized* networks are emerging to be the enabling technologies for future applications. The 5G networks, IoT Applications, MEC and Cloud services are leading to converged architectures (Figure 2). The ETSI specifies MEC as a *network service or chain of network functions* that can be deployed as an application in virtual machines/platforms or middleboxes. This SDNFV model provides a standard process to manage the entire life cycle of MEC services and a flexible dynamically programmable network. The research community has proposed reference architectures for enabling SDNFV in multimedia application networks [6]. From the literature survey, we studied the time, memory, and space complexity of various popular lightweight crypto ciphers. The advantageous methods of some ciphers were combined to form a new lightweight symmetric block cipher named *TREK*, specifically designed for 5G and IoT networks, which consist of high-speed forwarding elements and resource-constrained end-user devices. The proposed security scheme employs a simple dynamic key generation method that is computed from other fields of the packet header in network packet streams, variable session key, and hence this scheme is robust to modern attacks compared to other static-key based ciphers.

In this article, we focus on the security of the future 5G that is going to be developed from the integration of lightweight dynamically adaptable cryptographic cipher mechanism, application-aware dataplane fabric, and global authentication/orchestration controller to manage the security, as well as the QoE scheme. We propose a framework called *STREK* (*SDN* enabled *TREK* security scheme), which is designed to consider and optimize on multiple aspects simultaneously including monitoring, attack detection, network bandwidth management, data protection on communication channel in the Edge to Cloud networks. We also claim that our solution is one of the first SDNFV-based dynamic adaptable cipher security schemes for multimedia applications in IoT and 5G networks.

Some major contributions in this article are:

- We integrate our novel application-aware dataplane (DTARS [24, 25]) and secure SDN framework (VARMAN [42, 43]), from our prior works into 5G/IoT architecture to define a symmetrical, secure, and responsive communication channel at the edge MEC/Edge network for multimedia applications.
- Proposes a new multi-tiered *Cloud-to-Edge-to-Things_to_AP/UE* distributed TREK security scheme and network function management architecture for 5G infrastructure.
- Presents a new scalable distributed lightweight symmetric block cipher security scheme called TREK
- In 5G small cell multi-domain deployments, our novel group authentication scheme uses a prediction-based multicast method to install/update the keys on the Access Points (APs) of neighborhood cells, improving authentication efficiency during handover, avoiding unnecessary latency due to session re-establishment and fulfilling the 5G latency requirements.
- Network slicing, QoE-aware SDN design are enabled for 5G applications.
- A library of dynamically loadable Virtual Network Functions (VNFs) implements coordinated multimedia services and API for applications to dynamically enforce policies.

We show that our SDNFV-based STREK provides a greater level of quality distortion for multimedia contents without any encryption bitrate overhead. The SDN-enabled multimedia network delivers fairness in QoS to multimedia clients, and the encrypted communication channel is immune to static cryptanalysis, resistant to communication channel MITM, Jamming, Replay attacks, and adaptable for any media content. The multimedia and other advanced 5G applications can utilize the northbound APIs and SDN specific OpenFlow API/TREK SDK to programmatically define security and QoS policies, even at runtime.

The rest of the article is organized as follows: Section 2 gives a background of enabling technologies like 5G, IoT, Multimedia, challenges, and an overview of some popular works that addressed Security and QoE in 5G/Edge networks. Section 3 proposes our novel architecture and solution framework. Section 4 discusses the implementation. Section 5 presents the experiments and performance evaluation, Section 6 discusses the results, and Section 7 concludes this article.

2 BACKGROUND AND RELATED WORK

We provide a background to the enabling technologies for 5G networks and an overview of the challenges in 5G security. We discuss the relevant publications that addressed some issues in Quality of Experience (QoE) and the challenges in securing communication channel for multimedia applications, in the context of 5G/RAN/IoT modern networks. We also make a case for the role of lightweight cryptographic methods and enabling SDN to solve some of the hard problems in these ultra-low latency networks.

2.1 5G Security Architecture

We present an overview of the security issues in 5G deployments. Figure 3 provides a schematic view of the 5G architecture and depicts major security elements that are considered in the interconnected MEC and Centralized Cloud control model. The security automation that can manage holistically the overall orchestration of policies from applications to cloud to fine-grained edge level access control is the key requirement for future networks. The attack vectors in 5G networks

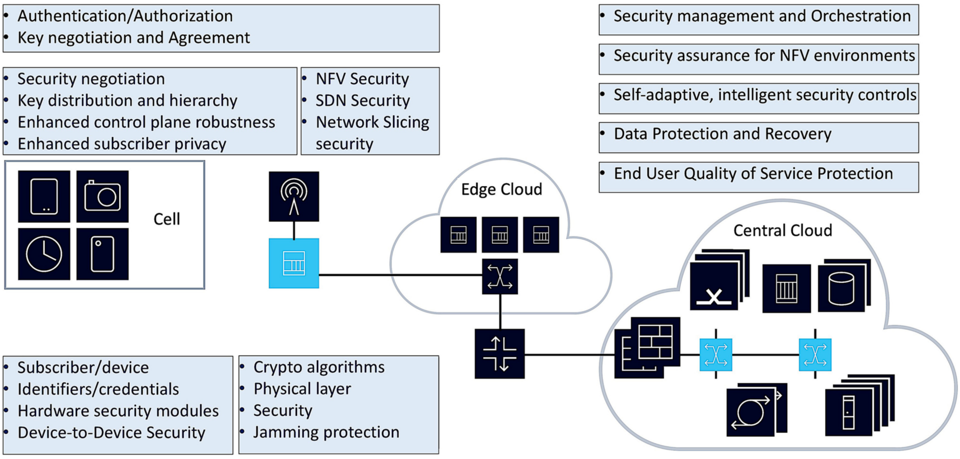

• Authentication/Authorization
• Key negotiation and Agreement
• Security negotiation
• Key distribution and hierarchy
• Enhanced control plane robustness
• Enhanced subscriber privacy
• NFV Security
• SDN Security
• Network Slicing security
• Security management and Orchestration
• Security assurance for NFV environments
• Self-adaptive, intelligent security controls
• Data Protection and Recovery
• End User Quality of Service Protection
Cell
Edge Cloud
Central Cloud
• Subscriber/device
• Identifiers/credentials
• Hardware security modules
• Device-to-Device Security
• Crypto algorithms
• Physical layer
• Security
• Jamming protection

Fig. 3. Major elements of 5G security architecture.

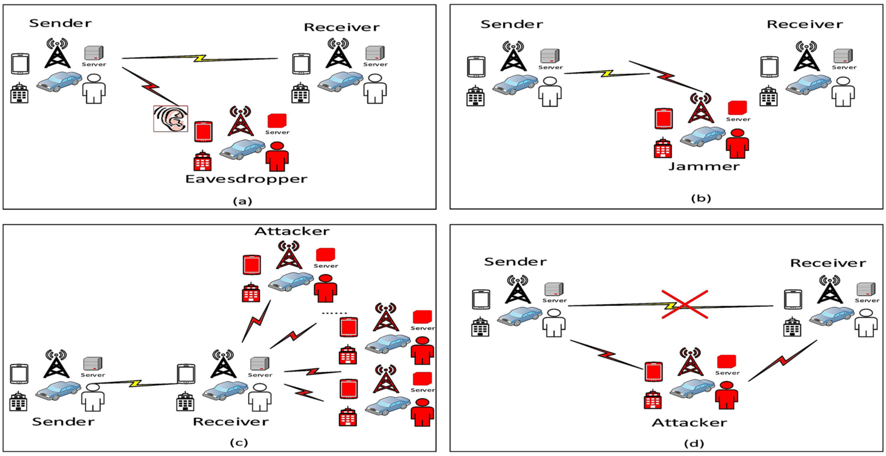


Fig. 4. Attacks in 5G networks: (a) Eavesdrop (b) Jamming (c) D-DoS (d) M-I-T-M [10].

are passive attacks (e.g., eavesdropping and traffic analysis, data confidentiality disclosure, user's privacy violations) and active attacks (e.g., man-in-the-middle (MITM), replay, Denial-of-Service (DoS) attacks). The two main approaches to defend these communication-channel attacks are through cryptography with new lightweight ciphers and physical layer security (PLS). In Figure 4, we illustrate the common attack vectors in 5G wireless networks. In this article, we primarily focus on data confidentiality service using lightweight cryptographic methods.

2.2 Data Confidentiality

Data Confidentiality refers to the protection of contents of messages from adversaries and only authorized parties can access the contents. The data transmitted over a communication channel (e.g., public Internet) should not be intercepted by adversaries, and even if the data are captured the adversary should not recognize or decode the information or reconstruct the encoded contents. The most reliable method to ensure confidentiality (also privacy) is by encrypting the transmitted message (from plain text to cipher text) that is on the wire and the cipher scheme should be strong enough that the attackers in the middle cannot do decryption within reasonable time and with practical computing resources at his/her disposal. The captured traffic data can be analyzed for patterns that will lead to insights, breach of privacy, and leaked intelligence, e.g., sensitive info, such as the sender's/receiver's location. Given the vast application landscape of 5G and IoT technologies, it is a daunting task to protect the privacy and confidentiality of billions of users' data (e.g., vehicle route, health monitor). Cryptographic mechanisms can be applied based on the context and are broadly classified as Asymmetric/Symmetric, Stream/Block ciphers, and they employ public/private keys to protect the data on the encrypted channel between the communicating parties. The legacy methods in cryptographic algorithms are designed assuming that the intercepting adversaries do not possess resources as sophisticated as the parties involved in communication. But the modern attackers and cybersecurity hackers' eco-systems have much more sophisticated tools and resources to break even advanced security schemes. So, the responsibility is on the network operators for deploying lightweight, trust-worthy, and secure communication channels and yet meet the QoS (Quality of Service) guarantee to the subscribers.

2.3 SDN for Multimedia Applications in 5G/IoT/Edge Networks

In Reference [10] the authors proposed a 5G wireless architecture for handover/signaling process, securing and utilizing the end-user identities for authentication. They further discussed the differences in 4G and 5G trust models, security schemes for D2D (Device-to-Device) communication and Heterogenous Networks in 5G. Generally, it might be thought that the full encryption of compressed video is required to protect the contents, but full encryption is often unnecessary, as Selective Encryption (SE) [11] reduces computation overhead while obscuring the video content. A novel SDN-based security coding scheme is presented in Reference [12] and the devices in the network path encode the packet streams that pass through. The controller monitors and manages the network, including the authentication of member devices that can participate in the coding scheme. The disadvantage is the accumulated encoding delay accrued when the packets have to traverse through multiple nodes. Ongaro et al., [13] present an SDN-based QoS management solution for real-time multimedia applications. The authors of Reference [14] introduce an SDN orchestration and control platform for multimedia distribution applications in 5G networks and the scope of their investigation is limited to QoS. Pencheng Liu et al. [15] presented a solution both in hardware FPGA embedded in OpenFlow switch and in software a lightweight PRESENT cipher scheme for securing multimedia streaming applications in SDN networks. Noura et al. [16] proposed a security scheme for authenticating multimedia contents, employing a *dynamic key-dependent stream cipher.* They claimed that their dynamic-key scheme is immune to existing cryptanalysis techniques and attacks, that traditionally break static cipher schemes. Reference [17] presents the Service Virtualization Platform (SVP) architecture enabling SDNFV for delivering QoS to multimedia services in 5G platform and presented case studies in 3D multimedia. In Reference [18] the authors propose an SDN framework for videoconferencing applications in multi-domain cloud networks. In Reference [19], the authors tackle the multimedia authentication problem in 5G networks, with a general trust authentication framework using a novel scheme called "Trusted Content Representation (TCR)" for content protection and it is adaptable for both higher and lower layer protocol semantics. The authors of Reference [20] proposed a flexible design for "IoT MultiMedia (IoTMM)" applications and discussed data sharing, multimedia content classification at various levels (e.g., IoTMM device level, IoTMM-to-cloud, IoTMM-to-MEC-to-Cloud). Reference [21] presented a novel authentication in an SDN controlled 5G small cell network. As the subscriber's UE roams between the small cells, their scheme transfers the security credentials in a special manifest called "weighted secure-context-information (SCI)." Their design is claimed to be efficient in the 5G mobile network in terms of handover-delay between cells and they utilized queuing theory simulations to demonstrate their solution. Reference [22] proposed a lightweight cryptography scheme "elliptic curve signcryption" for Video surveillance network application, deploying small footprint protection mechanisms on camera devices and encrypting video streams for secure multi-camera/monitor network. In Reference [23], a "Chunk-Size Aware SDN-assisted DASH system (CSASDN)" is presented to deliver QoE in a high traffic public WAN. Shuai Zhao et al. [26] discussed a "Dynamic Adaptive Streaming over HTTP (DASH)" in the context of "Application-Aware Network (AAN)" and proposed the SDN-driven model for delivering QoE metrics, optimizing the network path costs, dynamically selecting the encoding schemes to offer efficient streaming services in cloud networks. The 5G-MEDIA research [27] proposed an approach integrating the NFV for "Function-As-A-Service (FaaS)" with the emerging *serverless computing* paradigm in the cloud service model. This project further provided the API/SDK for developing new multimedia applications and service platforms in the 5G networks. In Reference [41], authors proposed a dynamic resource provisioning algorithm for VNFs in Edge network, adapting to dynamically changing network volumes.

2.4 Lightweight Security for 5G/IoT Systems

To enable secure multimedia transmission over the public channels, we need to encrypt the multimedia data before transmitting it on the communication channel. The QoE parameters and security level vary with application classes. For example,

Video conferencing, telemedicine, surveillance applications: Need a high level of security and encryption effort. It can be achieved by employing transformation to every bit or byte in the code stream.

Digital TV broadcast applications: Security level and encryption effort are low such that the content must not be consumable by illegal users. It can be achieved by transparent encryption through which high quality of version has to be hidden and a preview image or video can be decodable even if the key is unavailable.

Pay-per-View, video-on-demand applications: Security level and encryption effort need not be high, need sufficient encryption, and about 10% of encryption effort is sufficient so the hardware and software effort is minimized to make the set-top unit cheap. The encrypted image or video content must not be perceptible.

In summary, the key requirements from a multimedia application encryption scheme are:

- playback quality should not be degraded (i.e., continuous playback is essential).
- end-to-end security on communication channel (i.e., streaming server to client app).
- footprint scalable and lightweight (deployable from workstations to switches to small devices).
- offset in the video stream (i.e., to fast-forward or rewind content without degradation).

The lightweight ciphers were introduced to fulfill the requirements for security computations in resource-constrained devices [28]. The cryptographic research community has been advancing this field and contributed a series of lightweight crypto designs, some of which are discussed in Reference [29], However, only a few have been used in practice and standardized by the ISO and IEC. In general, the symmetric cryptographic scheme is widely deployed, as the design is simple, with low computation, space, and memory complexity comparing to asymmetric methods. Recently, considerable research is advancing to improvise the block ciphers, AES lighter and installable on tiny-small form factor/power devices. The advantages of block cipher designs for streaming multimedia applications are: (i) Real-time delivery has stringent delay constraints—simple block operations provide the fastest encryption. (ii) As the video streams are bursty traffic, the variability

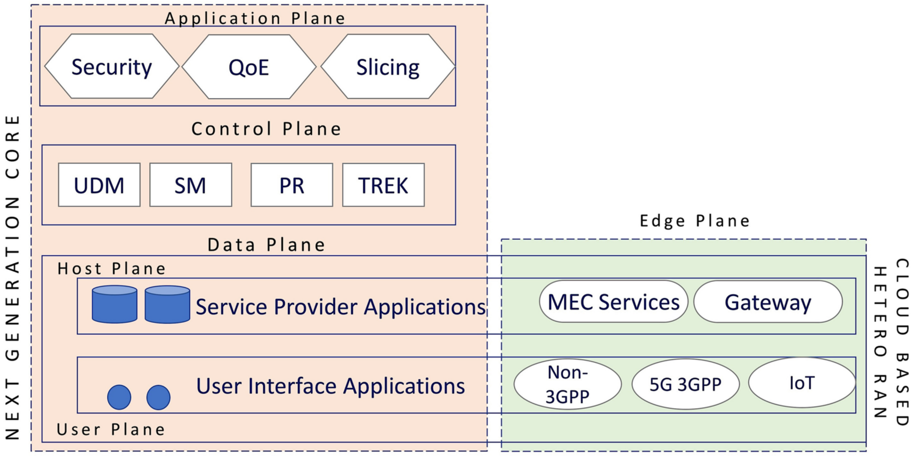


Fig. 5. Proposed STREK 5G network security architecture.

of block size helps in the synchronization of buffers. The “Substitution and permutation and Feistel networks (SPN)” proposed in Reference [30] are built with various functional blocks applied on plain text, looping in multiple rounds to form a network. Feistel network is built by applying invertible functions on plain text inputs for multiple iterations, using different key in each round. I-PRESENT [32] utilized the PRESENT cipher in its solution and presented the feasibility of the combination of SDN & PRESENT for video applications. PRESENT cipher was a significant breakthrough in lightweight cryptography, combining the salient functions of AES+DES. The plain data will iterate through the sequence of functions S-*box, P-layer,* and *Add-round key* to result in cipher-data. The completely wired diffusion characteristic is perfect for space-optimal implementation in hardware. Rectangle [33] is a lightweight cipher that used a slicing design to build an high-speed cipher and implemented in a resource-constrained system for high-performance applications. The architecture is derived from AES but has achieved a smaller size by replacing the matrix multiplication with bit permutations and resistant to attack until 18 rounds. KLEIN [37] proposed a block cipher that combines the AES Mix Column operations with 4-bit S-boxes and Substitution Permutation Network (64-bit blocks) for the encrypting scheme. ESPRESSO [35] is another lightweight stream cipher, proposed recently for 5G architecture and claims the lowest overhead and best QoS. Apart from the block and stream ciphers discussed above, we have focused on Rectangle cipher for its simple implementation and its similarity in structure with AES.

3 PROPOSED SDN-TREK FRAMEWORK

We present the architecture design and details of the major components of our framework.

3.1 Framework Composition

Figure 5 illustrates the proposed STREK architecture in a typical edge deployment. An SDNFV-driven framework is designed for 5G and MIoT applications, with open standards so that any application or network can be integrated into this model.

- Application Plane: Applications are deployed to monitor and drive dynamic traffic shaping and security access control policies. The parameters are passed through the northbound API.
- Control Plane: Key management and creates a time-expiring key where the key expires after a certain time interval. This central system consists of these key functionalities:

  - **MEC Services (MEC):** to manage multiple access protocols and mobile services.
  - **Session Manager (SM):** to enforce policies and control session of subscribers.
  - **Key management:** distribution, lease, recall, revoking of keys with devices.
  - **Unified Data Management (UDM):** to manage subscriber's profile, logs in the 5G core.
  - Event scheduler.
  - **Device database:** VNFs run to discover devices and maintain a table with profiles.
  - **Policy Resolver (PR):** to translate the runtime parameters from applications to OpenFlow rules.
- **Flow management:** polling, monitoring, install, scrubber, flow tables on the switches.
- **Cross-domain control:** interface to other controllers in multi-clouds
- Dataplane: These are switches that have the capability of performing lightweight crypto operations. The TREK cipher can be deployed as an FPGA module or hardware circuitry.
- Edge Plane: This can be a wireless MEC controller, Access Point (AP) or 5G Base Stations or IoT Gateway. UE/clients can be connected through multiple access protocols (wireless/wired).
- Host Plane: The server needs to run a stateful protocol like Real Time Streaming Protocol (RTSP) so the SDN controller can use the session ID to issue new keys to the OpenFlow switches. Stateless protocols like HTTP servers can also be used, but the packets would have to be modified to include session information that can be interpreted by the OpenFlow switches so they can identify the beginning of a new session. The server also uses end-to-end encryption with TLS.
- User Plane: User equipment, mobiles, smart devices, IoT sensors, vehicles, drones, and so on. These are the endpoints or clients or subscribers that consume the data stream. These clients are capable of performing end-to-end encrypted communication protocols like TLS.

3.2 SDN Architecture

The reference specification [9] for SDN architecture had defined the roles and abstractions of control/dataplane layers, with OpenFlow as the de facto control channel communication protocol. The key improvements that we have contributed to the classic SDN architecture and the Open source stock OvS SDN software stack are summarized here.

Control Plane: The controller extensions are designed using the *Vendor actions* message type, as specified in the Openflow protocol. This is a multi-threaded software package that consists of modules to handle the service upcalls from the southbound channel and northbound API from applications. It processes the in-band OpenFlow protocol and topology discovery/management messages and out-of-band alerts of malicious or suspicious flows. The STREK coordination and Unified STREK API exposes a northbound interface to services and applications.

Dataplane: This is where packets/flows carrying data over the networking/application protocols are exchanged in the interconnected network. The key elements are OpenFlow switches, specialized appliances/middleboxes, Ethernet L2/L3 switches, and routers, 5G/4G Base stations/APs, MEC Gateways (e.g., IoT, Wi-Fi). In STREK-enabled network, we will upgrade the appropriate devices with STREK dataplane stack to integrate our solution framework for the applications. The flow-table format is extended to include STREK and Handover keys (both per-flow and session), session-based timer (keys expire after the lease period), and TREK security flag (enabled or disabled by controller/application through a flow-rule update).

We have extended upon the stock "Open Virtual Network (OVN)" technology source base and created our customized SDNFV stack, ported and tuning done to interface with ETSI-compliant MEC 5G services software pieces. We have implemented modifications to the Open vSwitch (OvS)

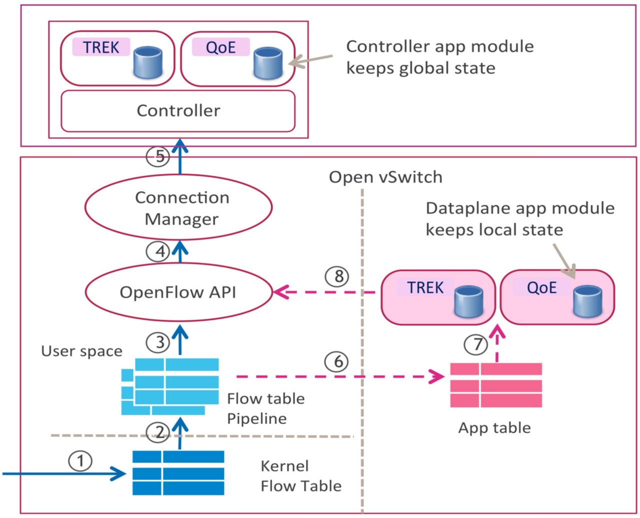


Fig. 6. Application-aware SDN architecture.

dataplane in IoT/MEC gateway routers or core switches and enhanced the controller, and together they form the SDN stack of STREK enabled network. Figure 6 shows our novel application-aware SDN stack (designed as part of our prior paper [24]) and the full path of a network packet until it reaches the controller.

The switch stack has two internal layers: One phase of functions run in the KERNEL space, and the second phase runs in the USER space. The red arrows (Steps 6–8) show the detoured workflow of the packets through the stateful application-processing components of the dataplane (switch). In our modified SDN stack, the controller installs the application-logic into dataplane, the switch changes the original *table-miss* rules and substitutes with *goto application-pipeline* instead of *goto controller.* During runtime, if a new flow arrives at a switch, the switch will generate a PACKET-IN message for the first packet of the flow. The controller will add stateful table entries to the switches according to the application logic. The application can set up new policies through the controller, which will install a new flow rule (e.g., "*dst_ip = x, tcp, dport = 80: fw, qoe, trek, install*") on the switch, which will then update the flow table with an entry in the "action" field of the match rule. The STREK framework is realized with this *application-aware SDN stack* at the core and provides a development environment that includes SDK, Switch Abstract Interface (SAI), application library, packages to program application-specific VNFs, and interface to customize the service-chaining in SDN-enabled MIoT/Edge networks.

3.3 Operational Overview

The multi-domain SDN-TREK cloud framework we deployed is illustrated in Figure 7. The TREK scheme is realized within the OpenFlow pipeline through the Security-enhanced *match-action* operations. With the SDN flow-based network routing, the flow tables on switches (right from the source to destination) and all the intermediate routing switches that participate in the Openflow control protocol can be configured to apply specific policies on all the packets of any particular flow. This configuration can be programmed in the applications through the SDN controller API and enforced autonomically by the controller on all the switches in the cloud and private networks. In the context of secure communication channel for end-to-end data confidentiality service, the TREK-enabled cryptographic application deployed in the SDN Openflow compliant switches/APs will encrypt/decrypt using the associated scheme and key for the matching flows. The network

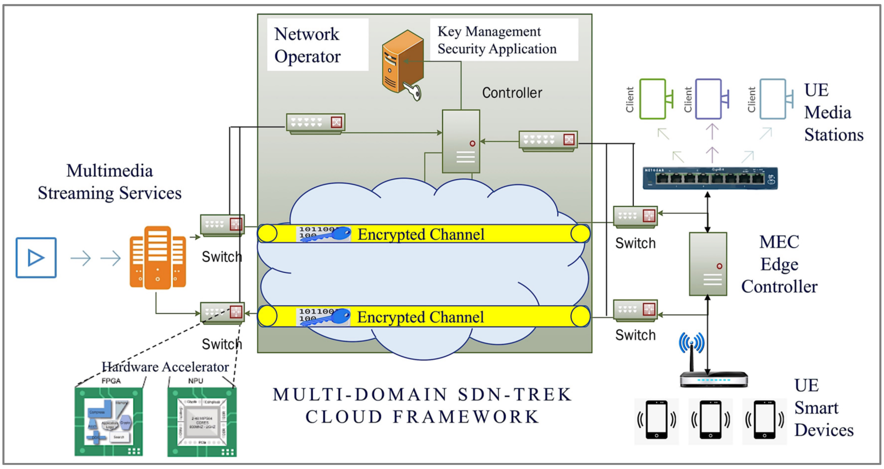
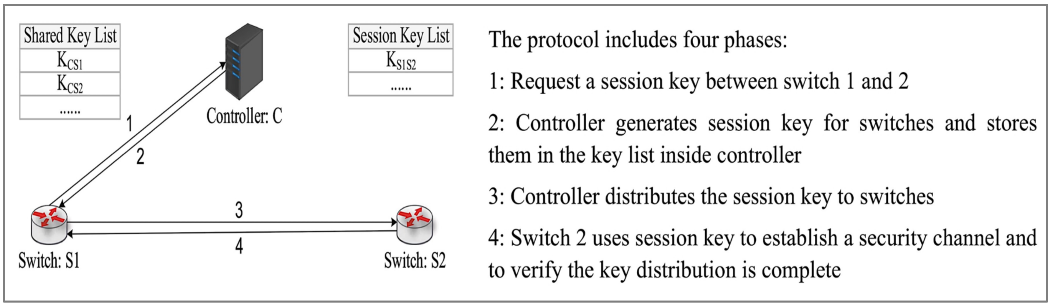


Fig. 7. STREK—SDN enabled TREK framework for multi-domain 5G/MEC/Cloud network.



The protocol includes four phases:

1: Request a session key between switch 1 and 2

2: Controller generates session key for switches and stores them in the key list inside controller

3: Controller distributes the session key to switches

4: Switch 2 uses session key to establish a security channel and to verify the key distribution is complete

Fig. 8. STREK crypto key distribution protocol.

protocol metadata headers are not encrypted/decrypted, so the traffic engineering and network routing functions are not modified; they work as per the open standards of the SDN operations. In the crypto-based scheme, the keys generation, distribution and management functions are very critical and so, they cannot be compromised. Also, the scheme has to make sure the switches and devices in the SDN-TREK network are all authenticated/attested at the time of joining the network. To ensure that the switches do not turn rogue at runtime or taken over by adversaries, the keys for the sessions are generated by the secure Controller with lease periods, refreshed periodically, also with random identity authentication scan (challenge/response technique to maintain the integrity of the network. The multimedia application servers, proxy services, multicasting devices, and the client end-points are authenticated at the time of joining the network and during active sessions. The clock synchronization and caching functions across the global SDN network, including the cloud-based controllers, and forwarding devices across the dataplane are managed by the central STREK controller.

Figure 8 shows how the TREK keys are securely distributed in the SDN network. We leverage on the OpenFlow standard SSL/TLS and Kerberos protocol for control channel security and across the multi-domain SDN Cloud network. We employed different protocols during the life-cycle of STREK sessions: (1) For Full Authentication with the home network and Initial STREK key distribution; (2) For Handover/Roaming Authentication with the service/roaming network.

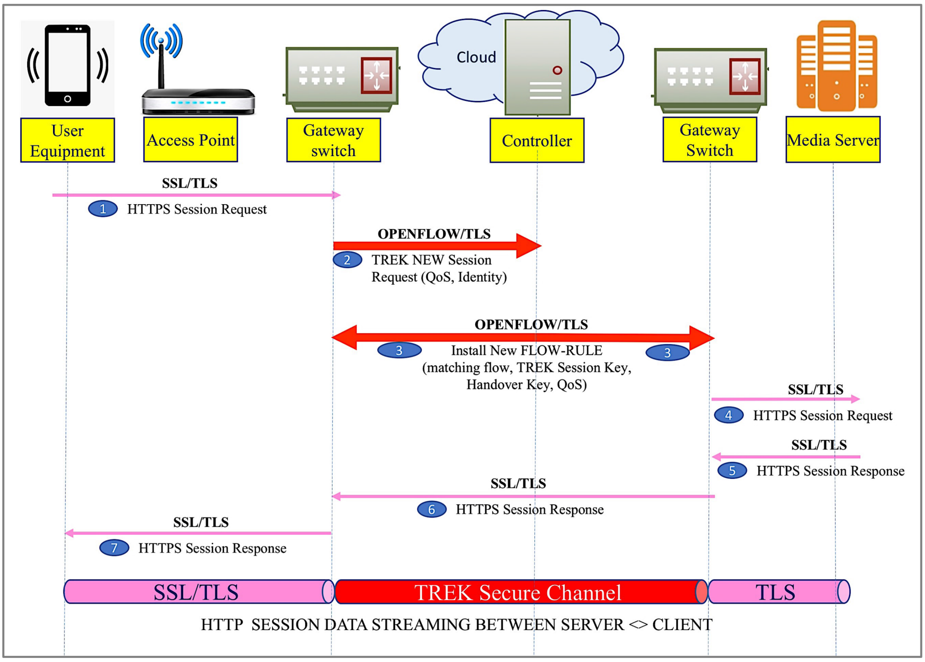


Fig. 9. HTTP session sequence diagram in STREK.

Initial Full Authentication: The TLS protocol, X.509 certificates, and Public-Key-Infrastructure cryptosystem were used to provide authentication, encryption, integrity, and non-repudiation using public and private key cryptography and digital certificates; It is designed to secure the two crucial phases - 1. Initial Full Authentication and 2. the STREK session key distribution. It also secures the control messages of the OpenFlow protocol between the Security Controller and the switches on the data plane. The TLS protocol through full encryption provides resistance from eavesdropping and data tampering.

Roaming Authentication: The Kerberos protocol provides a distributed authentication service for verifying principal identity over non-secure lines. On the communication channel, it sends a *hash-of-user-password and timestamp* and verifies at end-points by using the passwords as keys for encryption/decryption. The general assumption is that the end-point systems have time-synchronization with common network time services and the Kerberos ticket (short-lived session access permission) will be valid for user authentication.

As the Kerberos has a *single sign-on* authentication model, the users are expected to log in one time to access authentication services. Kerberos provides the cross-realm authentication, and this provides a benefit for the User/UE to simultaneously authenticate for a cluster of servers distributed across multiple domains/cells in each cell/roaming network. The SDN controller will host the key and ticket managing services. Kerberos communication is generally resistant to eavesdrop/replay attacks.

The block diagram and sequence diagram (Figure 9) explain the life cycle of a packet entering the SDN-TREK network from the application and leaving the network to reach another end-point.

The steps in the workflow are:

1. The packets arrive through one of the ports on the switch and the application reads the session information to determine whether that packet is a part of an existing session or a new session.

2. If the packet is a part of a new session, then the switch sends the packet (or just the header of the packet for low latency applications) to the SDN controller. The controller analyzes the packet and finds out the destination(s) of the packets (there can be multiple destinations in case of a multicast stream). Depending on the type of application that the packet belongs to, the controller decides which type of encryption scheme is to be used by the OpenFlow switch.
   (a) For example, if the packet is of an application that requires low latency (e.g., gaming stream), then it instructs the switch to use an encryption scheme like TREK, which is a low-latency scheme.
   (b) Otherwise, if the packet is part of an application that requires high bandwidth and can handle reasonable latency (like an FTP application), then the controller instructs the switch to use an encryption scheme like AES, which is a more complex encryption scheme (and hence slightly increases latency).
   (c) The controller creates a time-expiring key with the lease-period and installs the flow rules to the sending and receiving switches. The sending and receiving switches then update the match-action rule in their flow-tables, which store the key corresponding to a particular session.
3. If the incoming packet is of an existing session, the switches would already have the key stored in their table and hence would not have to contact the SDN controller. Therefore, the latency is considerably reduced.

Figure 9 shows the sequence diagram of how STREK establishes the end-to-end secure channel for HTTP communication and Media Streaming services across a public insecure cloud network. We leverage Open Standards-based OpenSSL/TLS (Secure Sockets Layer/Transport Layer Security) for the local network (Edge LAN) and the highly secure TREK secure protocol for media data transmission. The management/control channel between the SDN controller-switches will be based on the standard OpenFlow security protocols. We illustrate how the packets flow in this SDN-TREK cloud network, end-to-end packet exchanges for accessing a VIDEO streaming service over the HTTP protocol. First, the client(s) request a particular data stream and then the server replies to that request.

3.4 TREK CIPHER–based Security

TREK cipher is a lightweight cipher with an 80-bits key and 64-bits block size. The cipher is designed with 20-rounds Substitution and Permutation Network (SPN). We have used *involutive Sbox*, which reduces hardware size while implementing both the functions (encryption/decryption). Here the bit permutation is replaced by block shuffling, which provides better diffusion. It gives a better performance in hardware in terms of throughput. It can be implemented in low-cost hardware. Key whitening is used, where the input plaintext is XORed with an input key before the SPN.

From the experience of our previous work [3], we began the design of TREK cipher combining the advantages of *involutive Sbox* [38], reduced hardware, block shuffling, and an improved diffusion. The use of a *round constant* in key expansion provides security against self-similarity attacks. It is proposed to have better performance and smaller hardware than Rectangle cipher and Klein cipher. TREK is designed with dynamic lease-based session keys and hence resistant not only against self-similarity and brute force static attacks but also immune to sophisticated adversarial attacks. The workflow and stages of the TREK Encryption process are shown in the block diagram Figure 10.

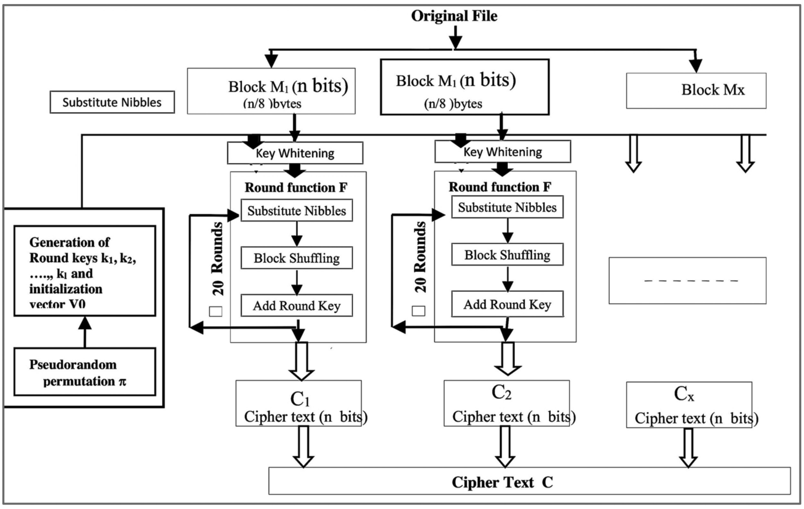


Fig. 10. Overview of TREK encryption process.

3.5 SDN-enabled 5G Authentication Handover

Ensuring service mobility is an important feature where optimal end-to-end session connectivity needs to be maintained for the entire course of the service usage. In the context of modern interconnected world, a phone or IoT device or smart vehicle move from home network to another service network (frequently changing the anchor points such as edge server or base station or AP) the MEC/5G service provider should ensure the QoE, and it is more challenging for low-latency applications. The *handover/handoff* is a phase in cellular communication where user sessions are transferred from one cell to another without service disruption. 5G specifications promise Ultra-Low Latency Reliable Communications (ULLRC). 5G Handover authentication should help users to securely roam across different small-cells/macro-cells. However, the complexity of the *handover* algorithm results in greater overall communication and computational overheads and hence this is a heavily researched practical problem in the 5G space. Existing classic handover authentication scheme faces challenges in robustness, un-traceability, computational, and communication overheads. These schemes always need to access the core/home network to facilitate handover. Hence, new lightweight solutions that facilitate graceful and un-interrupted handover experience (sessions managed locally at the remote/roaming cell station with lower latency) are a necessity.

Our novel inter-domain handover scheme (Figure 11) uses a prediction-based multicast method to install/update the keys on the Access Points (APs) neighborhood cells. The group of small-cells (Base stations /Access Points/Edge nodes) are configured from the home network itself, before even the mobility into other service networks takes place. This approach offers seamless session transition and uninterrupted transmission when the roaming begins for real-time multimedia application. The UEs require core network access only once for initial user registration/authentication and no changes in existing hardware infrastructure. The algorithm and the design parameters are described in Figure 12. The STREK establishes a TREK session-key and a handover-key (*H-key*); these unique session credentials are updated in the flow-rule, to be installed on the STREK switch at the entry point into the home network. This *H-key* is generated one time for a session and is a unique fingerprint comprising one/all of these attributes—subscriber home network USIM, MAC address of the UE, nonce, any protocol option field.

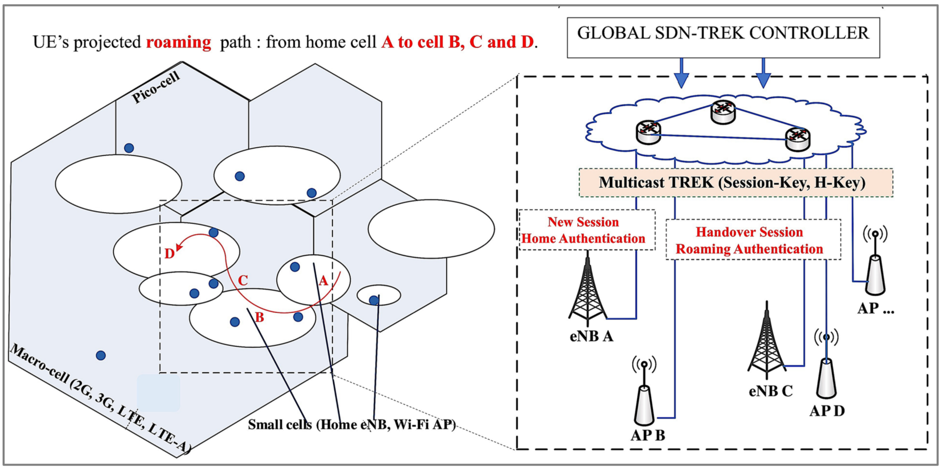
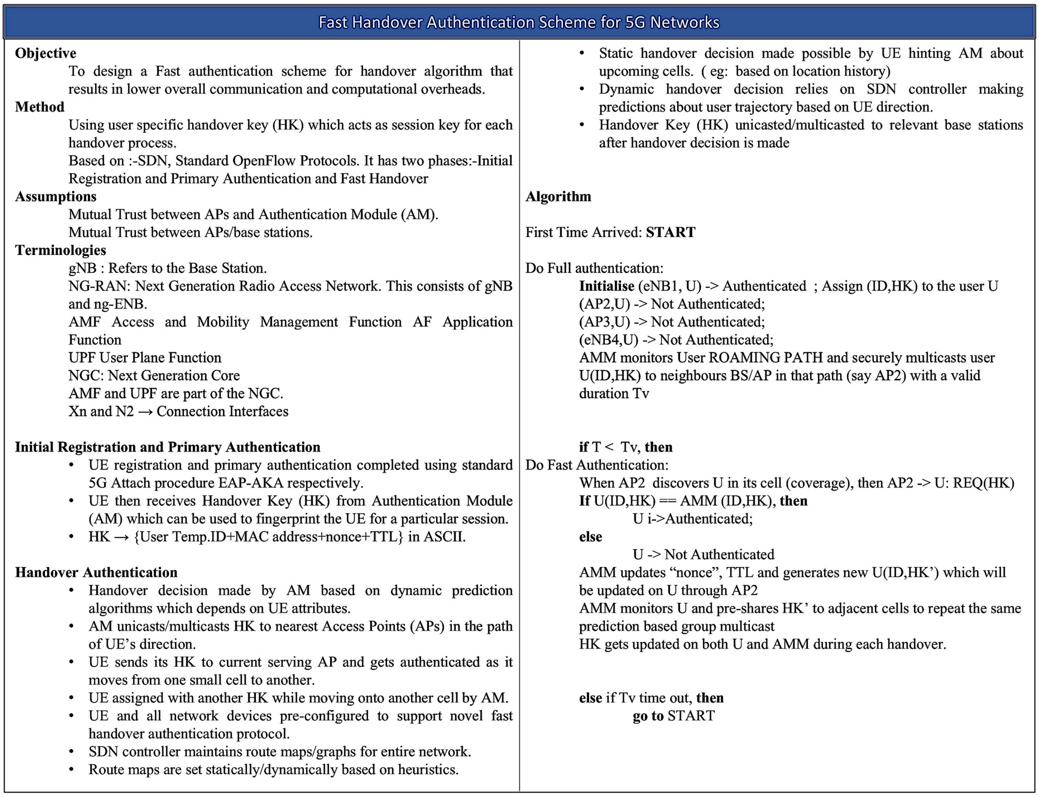

UE's projected roaming path : from home cell A to cell B, C and D.
GLOBAL SDN-TREK CONTROLLER
Pico-cell
Multicast TREK (Session-Key, H-Key)
New Session
Home Authentication
Handover Session
Roaming Authentication
D
C
A
B
eNB A
AP ...
eNB C
AP D
AP B
Macro-cell (2G, 3G, LTE, LTE-A)
Small cells (Home eNB, Wi-Fi AP)

Fig. 11. SDN-enabled secure handover scheme for 5G Mobility.



Fast Handover Authentication Scheme for 5G Networks

Objective

To design a Fast authentication scheme for handover algorithm that results in lower overall communication and computational overheads.

Method

Using user specific handover key (HK) which acts as session key for each handover process.

Based on :-SDN, Standard OpenFlow Protocols. It has two phases:-Initial Registration and Primary Authentication and Fast Handover

Assumptions

Mutual Trust between APs and Authentication Module (AM).
Mutual Trust between APs/base stations.

Terminologies

gNB : Refers to the Base Station.
NG-RAN: Next Generation Radio Access Network. This consists of gNB and ng-ENB.
AMF Access and Mobility Management Function AF Application Function
UPF User Plane Function
NGC: Next Generation Core
AMF and UPF are part of the NGC.
Xn and N2 → Connection Interfaces

Initial Registration and Primary Authentication

- UE registration and primary authentication completed using standard 5G Attach procedure EAP-AKA respectively.
- UE then receives Handover Key (HK) from Authentication Module (AM) which can be used to fingerprint the UE for a particular session.
- HK → {User Temp.ID+MAC address+nonce+TTL} in ASCII.

Handover Authentication

- Handover decision made by AM based on dynamic prediction algorithms which depends on UE attributes.
- AM unicasts/multicasts HK to nearest Access Points (APs) in the path of UE's direction.
- UE sends its HK to current serving AP and gets authenticated as it moves from one small cell to another.
- UE assigned with another HK while moving onto another cell by AM.
- UE and all network devices pre-configured to support novel fast handover authentication protocol.
- SDN controller maintains route maps/graphs for entire network.
- Route maps are set statically/dynamically based on heuristics.
- Static handover decision made possible by UE hinting AM about upcoming cells. (eg: based on location history)
- Dynamic handover decision relies on SDN controller making predictions about user trajectory based on UE direction.
- Handover Key (HK) unicasted/multicasted to relevant base stations after handover decision is made

Algorithm

```
First Time Arrived: START

Do Full authentication:
        Initialise (eNB1, U) -> Authenticated  ; Assign (ID,HK) to the user U
        (AP2,U) -> Not Authenticated;
        (AP3,U) -> Not Authenticated;
        (eNB4,U) -> Not Authenticated;
        AMM monitors User ROAMING PATH and securely multicasts user
        U(ID,HK) to neighbours BS/AP in that path (say AP2) with a valid
        duration Tv

        if T <  Tv, then
Do Fast Authentication:
        When AP2  discovers U in its cell (coverage), then AP2 -> U: REQ(HK)
        If U(ID,HK) == AMM (ID,HK), then
                U i->Authenticated;
        else
                U -> Not Authenticated
        AMM updates "nonce", TTL and generates new U(ID,HK') which will
        be updated on U through AP2
        AMM monitors U and pre-shares HK' to adjacent cells to repeat the same
        prediction based group multicast
        HK gets updated on both U and AMM during each handover.

        else if Tv time out, then
                go to START
```

Fig. 12. Algorithm of the fast authentication scheme for 5G handover.

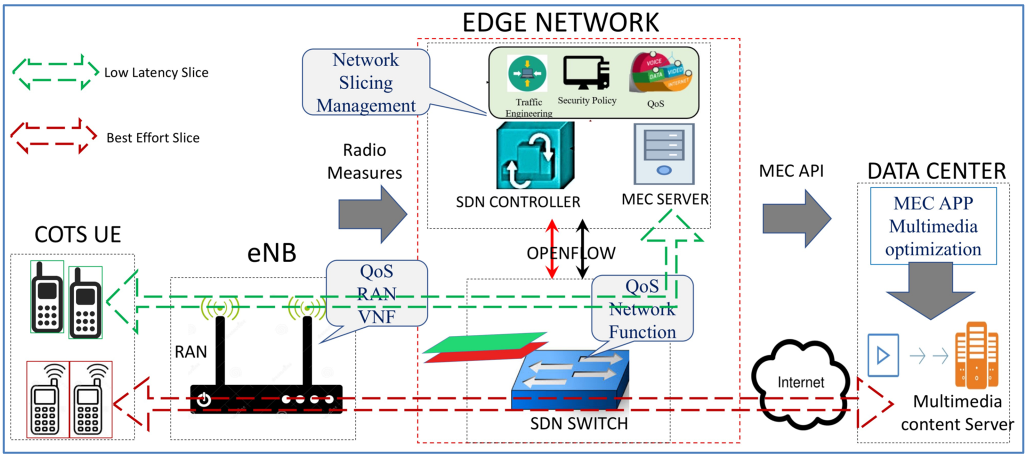


Fig. 13. STREK-enabled multimedia network slicing.

At the session setup time, for multicast streaming applications a multi-cast IP address/subnet is established at the network layer (e.g., IP multicast or broadcast) for the streaming server and it's clients. Based on the historical analysis of geolocations traversed by the UEs, we leverage on forecasting techniques to predict the routing path, establish a multicast-group consisting of the cells in the vicinity of the home cell, and multicast this *H-key* to the base stations or Access points or gateways or STREK/Openflow compliant standard switches. This phase prepares the entire 5G macro-cell (i.e., cluster of small cells) with the necessary credentials at the handover phase when the UE roams during the active session. Though this technique consumes extra space in the flow-tables of the cells and also adds some key sharing traffic across the large 5G network, the advantages of session continuity and seamless transition experience during live real-time multimedia session outweigh the additional overhead and resources. This *H-key* is applicable only to those UEs that have originated from/to a STREK networks and it is an optional feature. The other non-STREK UEs follow full authentication protocol in 5G handover and are independent of STREK session control. A suitable tunable parameter/active-lease period is provided for this handover/session-failover feature and during this period the mobility of the UEs is handled by this STREK cross-domain/cell authentication scheme automatically, without the intervention of the users or the interruption in the user service/experience.

3.6 Network Slicing

Slicing is a key enabling technology for 5G infrastructure in the network virtualization paradigm, similar to the SDN and NFV architectures. The SDNFV model offers an interface/API to program the network, slice and dice according to the requirements of co-existing applications and connected users to the services. A 5G network slice is a partition of a sub-network, with a bunch of user equipment (UE), applications, services, and physical switching systems configured with policies to meet the demands of that slice with best efforts. These parameters can be dynamically updated according to the traffic conditions and administrative policies of the physical infrastructure. We designed a network-slicing architecture for multimedia applications in the SDN control plane that analyze the flows, including the loads on the cells and real-time streaming (e.g., video buffering or freezing), and QoE parameters in each virtual network slice.

Figure 13 illustrates the enablement of network slicing feature by STREK in the context of MEC. The applications actuate appropriate tuning in the agent VNFs running in the dataplane switches and modify the action fields for the matching flows (e.g., adjust content quality via transcoding), thereby improving network efficiency. MEC platform mechanisms capture the congestion/channel quality events and send triggers to the optimizer module, which then fine-tune the streaming servers. The following are the key features:

- Video optimization application, being aware of the radio conditions in the cell.
- MEC applications co-hosted in base-stations(RAN), collaborating with multimedia content servers.
- Proximity of MEC Applications at the Edge.

The hardware-accelerated programmable dataplane is designed with feedback mechanism from network to applications, for dynamic fine-tuning of session settings. The runtime control is exposed to applications through the REST API for selecting policies on traffic that pass through the STREK switches. We implemented a Multi-Queue arbitration function to slice and manage multiple low latency communication channels for real-time streaming applications.

4 IMPLEMENTATION

SDN-TREK framework is designed with open standards. We choose to implement in software with diverse code-base, API, and also as a NetFPGA hardware switching system. We demonstrate some exemplary applications for content-aware server selection, load-balancing, network-slicing, Encrypt/Decrypt, NAT, GTP/4G-LTE Tunneling services in the SDN-TREK framework. The implementation scenarios have the choice of deploying software/hardware OVS-stack or both, and we have packaged SDK for this framework. In STREK framework stack, to expose a unified API to controller applications, we have designed the Unified STREK Access Interface (USAI) as a kernel device driver/module that can be installed on a controller-machine or *Whitebox* switch or *Edge server.*

4.1 SDN-TREK in Software

We adopted the Open vSwitch (OvS) from the opensource. The key functionalities such as: Session key distribution, management and TREK cipher functions are deployed in the OvS switch pipeline as *match-action* flow rules. The SDN architecture is built with customized Open vSwitch as the dataplane in 5G base-station/AP, IoT gateway, and an augmented controller package and 5G Crypto/QoE applications.

4.2 SDN-TREK in Hardware

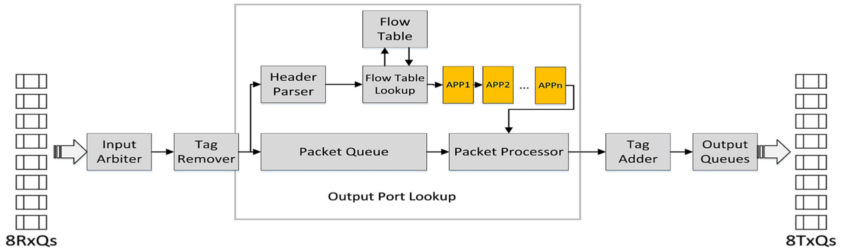
We choose the ONetCard acceleration, NetFPGA-1G platform to develop the SDN-TREK framework. The switching system supports multi-network ports, low-power CPU, and high-speed memory for TCAM OpenFlow 1.5x flow table and TREK cipher keys storage. Figure 14 illustrates the switch pipeline and the extensible architecture to dynamically load application modules/VNFs. The QoE applications and the TREK crypto algorithms are deployed in switch OF pipeline as NFs/Apps.

5 PERFORMANCE EVALUATION

We evaluated the SDN-TREK framework in representative practical multimedia use-cases and scenarios. The testbed is set up with the following major components:

SDN Stack: Ubuntu 16.04, custom OpenvSwitch (Modified OvS 2.8.x, Openflow1.7.x), RYU controller

Networking: Wi-Fi-enabled IoT devices, *Mininet-WiFi* to emulate IoT nodes, TinyCore Linux 3.16.6 for emulating a Thing (IoT), Edge Switches run OVS and MEC/IoT Gateway run the full MEC/SDN stack.



The hardware packet processing pipeline is composed of seven stages:

(1) RxQs input queues: buffering packets received from the Ethernet physical ports and DMA virtual ports.
(2) Input Arbiter: selecting one input queue through polling and dealing with that queue.
(3) Tag Remover: detaching the VLAN tag from original data packet.
(4) Output Port Lookup: core module for packet processing inside which the packets are temporarily buffered in the Packet Queue and the Header Parser gets the header fields. The Flow Table Lookup module matches the packet headers against flow tables to find associated instructions. The Packet Processor deals with the packets according to the instructions, such as modifying the header fields, dropping the packet or setting output ports.
(5) Tag Adder: combing the processed packet with VLAN tags to form a complete packet.
(6) Output Queues: sending the packet to relevant output queues on the basis of the processing decisions of the packet.
(7) TxQs Output Queue: buffering the output queue to output port.

Fig. 14. Hardware processing pipeline in TREK switch system.

Table 1. Performance of HTTP Media Streaming

FILE TYPE	FILE SIZE	Average Encrypt Time (s)			CPU Utilization (%)			Memory Usage (%)			Average Bandwidth Utilization (%)			Congestion level		
		AES	**REC**	**TREK**	**AES**	**REC**	**TREK**	**AES**	**REC**	**TREK**	**AES**	**REC**	**TREK**	**AES**	**REC**	**TREK**
Text	17 KB	0.09	0.05	0.023	40	40	40	36	38	38	42	42	40	0.50	0.50	0.20
JPG Image	115 KB	0.45	0.27	0.12	40	40	40	42	42	40	44	44	43	0.50	0.50	0.20
PDF Text	658 KB	2.05	1.48	0.60	48	42	42	44	43	45	47	45	45	0.50	0.50	0.22
PNG Image	1 MB	7.40	2.38	0.97	62	45	45	52	45	46	63	55	46	0.50	0.50	0.30
MP3 Audio	2.3 MB	9.54	5.21	2.05	96	90	50	91	85	48	96	95	60	1.10	1.10	0.65
MP4 Video	995 MB	3105	2216	867	99	99	65	99	97	69	160	130	97	1.30	1.30	0.99

MEC platform: OpenAirInterface (OAI) [31] a real-time 5G, LTE simulator package, Intel Linux workstations run the MEC platform and component services for the access network.

Crypto mechanisms: OpenSSL, Crypto++ and PBC libraries.

5.1 Software Stack

The TREK cipher and other security functions are deployed as VNFs in the SDN dataplane switch as part of the OpenFlow match-action flow tables. The encryption/decryption functions are thus made available to packets/flows passing through the SDN switch or AP gateway or on the Edge Node. Testbench system: Processor: Intel i7-6700HQ, OS: Ubuntu 18.04.3 LTS (64 bit).

The observations from the Table 1 (HTTP end-to-end streaming performance) and Table 2 (Encryption system efficiency), reveal the following for the TREK scheme: (a) Cipher(Encrypt/Decrypt) speed is faster, (b) startup delay smaller, (c) lower communication channel latencies, and (d) total bandwidth usage is less than peak value, even with congestions during a streaming session. The Congestion happens due to communication channel flooding. When the demands are

Table 2. Performance Comparison of Encryption System

PARAMETERS		AES			RECTANGLE			TREK		
Block Size		64	128	256	64	128	256	64	128	256
Rounds		10	10	10	10	10	10	6	7	8
Encryption time (ms)	25 MB	1,611	1,910	2,107	2,280	2,507	1,704	1,012	1,146	1,344
	650 MB	37,876	39,765	40,187	48,789	51,254	53,457	18,780	21,675	22,750
	1 GB	68,980	73,005	80,780	81,254	95,880	97,890	99,760	47,200	56,550
Encryption speed	KB/s	145.7	154.9	166	136	144.8	155	171	176.9	181
	Frames/s	22	30	36	20	28	36	35	40	45
Time Delay (ms)		31	36	46	35	45	50	21	22	24

Table 3. Performance in TREK Hardware

CIPHER TYPE	MAXIMUM COMBINATORIAL PATH DELAY	TOTAL TIME TO XST COMPLETION	SLICING	MEMORY USAGE(MB)	GATE EQUIVALENCEGE
KLEIN	133.91 ns	431 ns	76 %	402.98	2,629
RECT	55.31 ns	72 ns	20 %	321.64	1,570
TREK	39.61 ns	42 ns	14 %	320.63	1,350

greater than the available network bandwidth, violations occur. Any increase in congestions ≈1 is normal and values >1 represent network overloading.

5.2 Microbenchmark with TREK Hardware

For comparative analysis, we implemented the Rectangle cipher and its variant, Klein cipher, and our proposed TREK cipher in Verilog HDL, ModelSim and the synthesis was done on Xilinx Plan Ahead platform. In real-life deployment, the encryption/decryption circuitry can be built into the SDN switch/Access Point gateway or on the Edge Node.

Synthesis Report: The entire FPGA implementation process, design of RTL sources, synthesized netlists, resource utilization, interconnect delay, and routing connectivity are analyzed for improving the layout, floor plan of the circuitry. The ciphers are simulated with random bitstreams as block and key bits.

Table 3 shows the comparison of the parameters from the Xilinx testbench report after synthesis. The smaller values of "*maximum combinational path delay* and *total real-time to XST completion*" implies that the encryption process is faster in hardware.

Real-time to XST: time taken by the platform to run through the critical path.

Memory usage: memory used by the platform for the synthesis.

The reduced slice percentage proves that the cipher will have smaller hardware. The memory usage is also comparatively less. The Gate Equivalence (GE) measured equal to two-input NAND gates provides an estimate of the area required to implement the logic in hardware. Most low-power devices use only 10,000 GEs for the entire design and to secure these designs, cipher GEs are expected to be less than 2,000. There are standard encryption standards (AES) with 2,400–3,500 GEs and other lightweight ciphers with less than 2,000 GEs, but mostly they come with higher propagation delays and lower resistance to attacks. Based on our estimated GE, we have reduced 14% GE area with the TREK cipher when compared to another look-up-table and S-box-based cipher PRESENT [32]. It is evident from these results that the TREK cipher outperforms other popular lightweight ciphers in hardware performance.

Table 4. Correlation Coefficient

DIRECTION	PLAIN IMAGE	ENCRYPT IMAGE
Horizontal	0.9915	0.0509
Vertical	0.9811	0.0427
Diagonal	0.9836	0.0389

5.3 Security Analysis

The security analysis in the context of case studies relevant to our communication channel and capabilities in the 5G/IoT environment are summarized here.

Statistical analysis: The correlation calculation of pixels in the vicinity (horizontal, vertical, and diagonal axis) is done as follows:

$$\Gamma_{XY} = \frac{Cov(X,Y)}{\sqrt{D(X)D(Y)}}$$

$$Cov(X,Y) = \frac{1}{N}\sum_{i=1}^{N}(X_i - E(X)(Y_i - E(Y)))$$

Where $Cov(X,Y)$ covariance of X and Y, $D(X)$ variance of X, $D(Y)$ of Y, and (X,Y) denote gray-scale values of two adjacent pixels in the input data. The following discrete formulas:

$$E(X) = \frac{1}{N}\sum_{i=1}^{N}X_i$$

$$D(Y) = \frac{1}{N}\sum_{i=1}^{N}((X_i - E(X))^2$$

Linear Cryptanalysis: For us to perform differential and linear cryptanalysis, one must first calculate the linear characteristic over the Sbox $S(x)$. From Reference [33], we can conclude that the maximum probability of any output differential is up to $4/16 = 2^{-2}$. The well-known equation for the correlation of the linear characteristic of $S(x)$ is q = (2p–1)^2 (here we note p is the probability), one can easily determine that any linear correlation over $S(x)$ has at most $(2 * 4/16{-}1)^2 = 2^{-2}$.

Differential Attack Analysis: To prove the efficiency of TREK resisting cryptanalysis, we adopted the Sbox method (see Reference [36] for more details). In what follows, we denote P as the probability of a differential trial and N as the block length of cipher bits. The approach claims that it required P −1 < 2N attacks to recover keys and for TREK cipher to resist differential cryptanalysis, active S-boxes are bounded by $P^{na}_{max} < 2^{-N}$. Since TREK uses the same Sbox as KLEIN, we can apply the same Theorem as in Reference [33]. The theorem in this article states that any four-round differential characteristic of KLEIN has a minimum of 15 active Sbox. Since we have already shown that the max differential TREK is given by 2^{-2}, for TREK it is $(2^{-2})^{\mathrm{na}} < 2^{-64}$”. Thus, the cipher must reach minimum $\mathrm{n_a} = 32$ S-box for differential trials. The TREK algorithm has a minimum of 20 rounds thus, a probability for 20-rounds trial is therefore bound to $(2^{-2})^{20 \times 15/4} = 2^{-150}$. Thus, we can conclude that the keys cannot be recovered as $2^{150} > 2^{64}$ (i.e., the required number of chosen plaintexts exceeds the plaintext space).

From Table 4, it is observed that the correlations are much smaller in all axes for the encrypted image compared to the plain one. Figure 15 plots in two graphs on horizontal axes, the pixel correlations of (a) plain image and (b) encrypted image, to confirm that the plain image shows higher correlation than the image that passed through our TREK cipher encryption. So, we conclude that

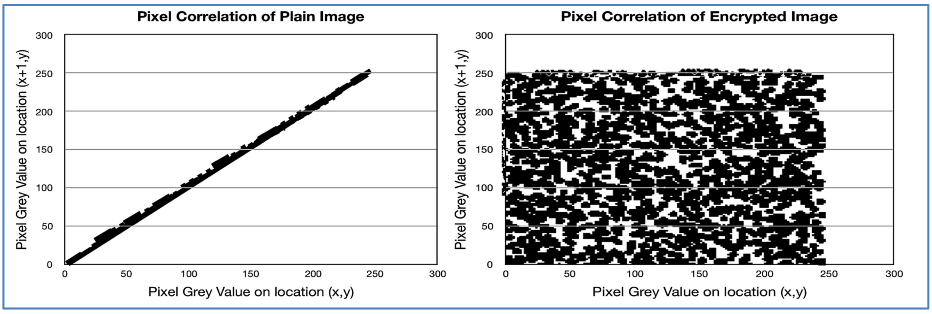


Fig. 15. Pixel correlation comparison.

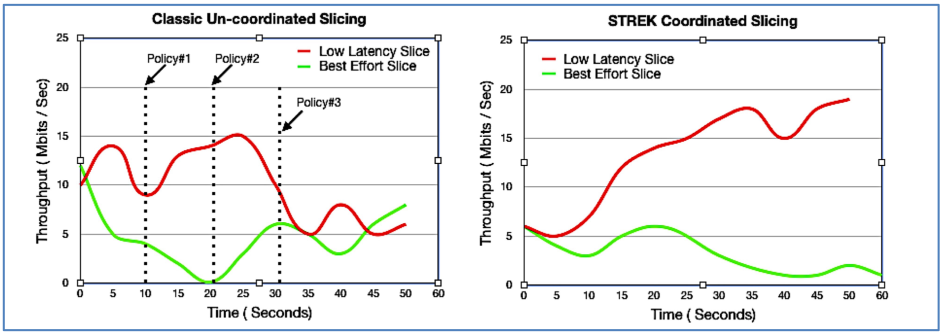


Fig. 16. Throughput performance with network slicing.

by statistical analysis the MITM attack/adversary will not elucidate the contents of the encrypted data through visual analysis or any exploits.

5.4 Demonstration of Network Slicing for QoE

We set up the slicing setup given in Figure 13 (Section 3.6), to demonstrate the realization of QoS features and an optimal resource utilization at runtime due to the dynamic policy enforcement application. We present two use-cases with a multimedia server streaming to its registered UEs on the SDN-controlled communication channel. Two slices were created consisting of one mobile user/User Equipment each. The fraction of RAN switching throughput per slice is determined by the respective policy. Both the slices demand different latency requirements, with MEC slice committed to serving the end-users with under-millisecond latencies to connect to the edge caching/proxy node and the Cloud slice can tolerate higher latencies to connect to the cloud main data center.

5.4.1 RAN Bandwidth Allocation. In this experiment, we deployed a slice policy enforcement algorithm for multiple RAN bandwidth allocation. Refer to the architecture diagram in Figure 13; we implemented a low-latency MEC program on the STREK control plane via the API. We created two slices and measured the switch bandwidth utilization, i.e., Plotting the throughput numbers (Figure 18) for normal setup (i.e., without network slicing enabled) coordinated setup (i.e., with STREK Network slicing enabled). From the results shown in Figure 16, we make the following inferences:

In Co-ordinated Network Slicing STREK enables dynamic shaping through the dataplane applications, and bandwidth policy changes are autonomically enforced.

Table 5. TCP throughput

Channel Quality Indicator(CQI)	Congestion Level	Download (Mb/s)	Upload (Mb/s)
0–4	High	1.10	0.70
4–7	Medium	5.78	2.65
7–9	Medium	10.80	4.90
9–11	Low	12.24	7.62
11–15	Low	16.23	9.02

Table 6. Handover performance

Features	3GPP	STREK
Mutual Authentication	Yes	Yes
Unique session key	Yes	Yes
User privacy	Yes	Yes
Communication Overhead	High	Low*
Computational Overhead	High	Low*

- The application monitors the utilization and enforces one policy change at time=15 s, to deliver two slices: (1) Best-fitting Cloud Slice; (2) Mbps, low-latency MEC Slice: 20 Mbps.
- *Low-Latency Slice* gets the data from the local MEC server (Green block arrow) and the *Best-Effort Slice* gets the data from the cloud data center origin server (Red block arrow).

In normal Uncoordinated Slicing, the bandwidth policy changes are manually enforced, and utilization is sub-optimal due to lack of feedback parameters dynamically from the RAN side (eNB) to Core Network. With STREK network-slicing scenario, due to co-ordination and runtime feedback from the RAN to CN and subsequent dynamic adjustments done by the SDN stack on the streaming-server side, we achieved the desired QoE results, i.e., different allocation based on priority and throughput requirements.

5.4.2 Variable Streaming Bitrate. We set up a MEC testbed, implemented a Dynamic Adaptive Streaming over HTTP (DASH) application in the STREK framework and appended a field in the switch flow table for tracking the "Radio channel quality indicator (RCQI)" combined with the cell congestion level to adapt the streaming quality, for each session flow to the end-user device/UE. When the UEs access the video stream, the STREK provides the following functions: (i) discovers an optimal network port/path to the least-loaded application server; (ii) sends *HTTP redirect* messages to that matched application client/server (e.g., Source/Destination-IP); (iii) fine-tunes the speed/bandwidth allocation in the flow-table policy for that flow, matching the predicted throughput of the client; and (iv) monitors the requirements of the UE sessions and load balances based on global view of stats from the dataplane. In Table 5, the CQI is mapped to maximum TCP throughput numbers, which proves that the variable streaming bitrates can be delivered by monitoring the flows on the network dataplane and establishing a discrete map between RCQI and switch bandwidth.

5.5 Fast Handover Authentication Scheme Analysis

The proposed STREK architecture is simulated in *NS3* with *LENA* and *mm-Wave* modules. The scheme is under investigation and early results are given in Table 6 comparing the standard system and STREK.

The handover overheads can be empirically estimated as follows:

1. Computation overhead at controller for UE trajectory prediction;
2. Communication channel overhead at the controller for executing the HK multicast algorithm (packet exchange between the controller to home switch and the group of switches in the roaming trajectory, predicted);
   Total overhead, $D = d_1 + d_2 + d_3 + \cdots\cdots + d_{n.}$ where d_n is the cost of forwarding the packets to the n^{th} switch.
3. Storage overhead at controllers, switches (extra space for additional flow rules in the flow table, action matching to the incoming UE);
   Total Overhead due to flow-table entries,
   $\propto(FE) = \{\propto(FE_1) + \propto(FE_2) + \propto(FE_3) + \cdots + \propto(FE_m)\}$
   where $\propto(FE_m)$ *is the* overhead due to $_m$th flow entry
4. Redundant overhead at the unused edge switches/base stations in the UE trajectory that received HK but could not serve the UE as it took a different path.

5.6 Attacks Simulation and Analysis

In this section, we present experiments that prove the resistance of STREK against malicious attacks such as replay attacks, Man-In-The-Middle (M-I-T-M) attacks, jamming/unknown attacks.

5.6.1 Resistance against Replay and MITM Attacks. The Replay attackers intercept the messages, hold, and retransmit them on the same communication channel. We employ the Kerberos authentication protocol, which ensures a *One-time Secure key(OSK) and timestamp* for each session and refreshed after the expiry of a timer. Refer to Figure 8 for the design. The three-way handshake protocol is performed for the initial sharing of a *One-time Secure key(OSK)* between the Controller and the participating nodes (e.g., 2 base stations and controller). Whenever a new session becomes active for data transfer, the nodes can validate the session with *nonce-challenge* messages and the probability of the same *nonce* generation is nil during the initialization of different sessions. Hence, we can claim that our authentication scheme will resist replay attacks. The M-I-T-M attackers tap the communication channel and tamper/corrupt the data going to the victim end-points. With the proposed TREK scheme, the communication channel is encrypted with *OSK*, and only the end-points can decrypt the data. Without OSK and the hash function, the attackers cannot corrupt the data. During re-authentication, since the roaming UEs do not transmit the clear password, adversarial replay, eavesdropping, tampering, or session hijacking attacks are not possible and thus, the STREK scheme is proven to be secure against any network-centric attack vectors.

5.6.2 Resistance against Unknown DoS and Jamming Attacks. As the attack vectors are growing, the newer attacks are not predictable and sometimes called zero-day attacks. We simulate various attacks such as flooding, jamming, and DoS, with various attack ratios. We compare the unmodified SDN and STREK framework in an attack simulation and application testbed.

Observations from the simulation results are plotted in three graphs (Figure 17):

- Authentication delay: This indicates the average handover authentication delay when the attack ratio is increased from 0.1–0.9. SDN defense mechanism has to do additional processing in the attack detection and failure handover authentication. We observe that the average authentication delay for STREK is about 1/9 of that of the classic SDN scheme.
- Packet Loss Ratio: It is the ratio of total packets sent and lost in the network due to congestion. The experiment shows that the STREK scheme has gradual loss but in standard configuration, the packet loss ratio spikes up over time.

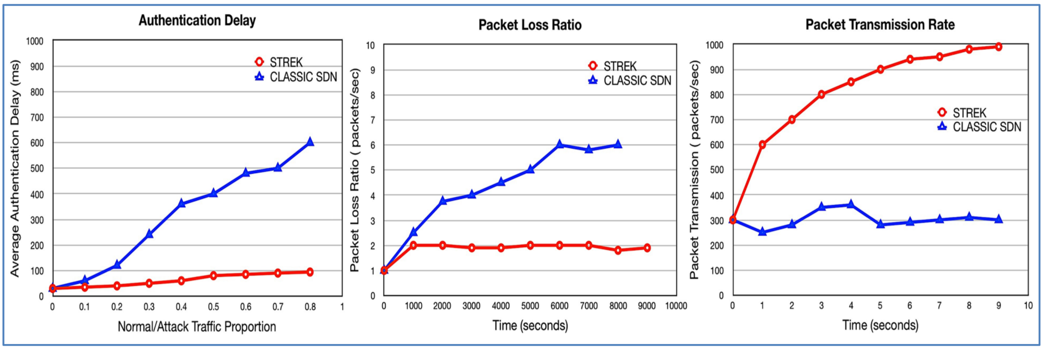


Fig. 17. Measurement of network performance.

- Packet transmission rate: This metric shows the ability of a network to transmit packets and sustain the throughput in the network dataplane during attack detection. The experiments show that under normal traffic conditions, STREK achieves a *Peak* rate of 1,000 packets per time-slot (20 Mbps). When the network is under DDoS attack, STREK sustains the *Average* rate of 750 packets per time-slot, but the standard configuration achieves only about 210 packets per time-slot.
- In STREK architecture, the defensive dataplane detects the DoS attacks and the security-VNFs deployed in the SDN stack prevent the application network from saturation.

Thus, in terms of key network performance and resilience metrics such as Authentication delay, throughput packet rate, and packet loss ratio, the applications that run under the STREK framework can achieve the guaranteed QoE without compromising the security.

6 DISCUSSION

In this section, we articulate some key observations from the experiments, comparisons to the other solutions, and potential extensions to address the limitations of the SDN/NFV-based solutions in general. In our solution, we have systematically studied, compared, and embraced the latest advances in designing the SDN-enabled framework for multimedia applications in future data-centric 5G/wireless networks. The key problems that happen in operations are (1) Dynamic control, optimization, and user mobility in large-scale networks and (2) Security of communication channel and authentication of users in low-latency 5G heterogeneous network, and we discussed how STREK addresses both. Table 7 presents the evaluation strategy and key findings in our experiments. The network performance, microbenchmarks, and computation complexity experiments, in practical application case studies, showed that the TREK security scheme incurs just reasonable overhead, outperforms the comparable lightweight ciphers.

7 CONCLUSIONS AND FUTURE WORK

Through this work, the key research question we have attempted to address is whether emerging SDN/NFV paradigms can offer dependable communication channel for modern multimedia applications. We intend to design an offloading-scheme for the low-power devices/UEs on the Edge and Small cells to offload the expensive security and computational tasks to the trusted Edge Nodes or Gateway routers in future multi-access edge computing and 5G Hetnets. Towards delivering secure multimedia application environment in the context of modern networks, the proposed Softwarized SDN-TREK framework has taken a significant stride to deliver a highly adaptable QoE and secure communication channel for media services in 5G/IoT networks. The key contributions of this

Table 7. Evaluations Summary and Key Findings

SECTION	ASPECTS	DISCUSSION
5.1 TREK Software Stack	HTTP end-to-end streaming performance	With SDN, the controller has a global view of traffic congestion and switches provide an agile re-mediation, path optimization scheme. We observe lower communication channel latencies and bandwidth usage is less than peak value, with intra-net traffic dynamics, jitters and congestions.
	Encryption system efficiency Cipher-Block chaining	Cipher speed is faster, and startup delay smaller. We improved upon the Rectangle cipher, smooth synchronization between sender/receiver, through effective use of block size and reducing rounds and the total number of blocks for the scheme. We see that for larger messages, this provides optimal chaining of blocks, slightly reduced performance but provides better security.
5.2 TREK Hardware	combinational path delay	The smaller values of "maximum combinational path delay, total real-time to XST completion, slicing percentage" imply a faster encryption process.
	Gate Equivalence (GE)	Based on our estimated GE, we have a 14% lesser gate equivalent area with the TREK cipher in comparison with other lightweight ciphers such as PRESENT, RECTANGLE-80, advantages for the low-power devices.
5.3 Security analysis of TREK	Pixel correlation co-efficient	The plain image shows higher correlations than the TREK encrypted image. So, with the statistical analysis, the MITM attack/adversary will not elucidate the contents of the encrypted data, through visual analysis or any exploits.
	Differential Analysis	We concluded that the keys cannot be recovered as the number of chosen plaintext exceeds the required space. Other statistical and linear analyses also validate that our TREK scheme is fully robust and resistant to any practical MITM attacks in the communication channel and thus feasible to apply in real-time multimedia and interactive applications on the public internet.
5.4 Network Slicing for QoE	QoS features and dynamic resource utilization	In Co-ordinated Slicing STREK enables dynamic shaping through dataplane applications and bandwidth changes are autonomically enforced. In Uncoordinated Slicing, bandwidth policies are manually enforced, utilization is sub-optimal due to lack of feedback from the RAN to the data network.
	Variable Streaming bitrate and throughput	When UEs access multimedia applications in real-time, the STREK will slice and shape the speed/bandwidth allocation in the flow-table with the predicted throughput of the client and monitor the requirements of the UE sessions and load balance based on intelligent traffic flow analysis in the dataplane.
5.5 Authentication	Handover overheads in 5G small cells	The handover overheads are empirically estimated, and early results show better performance in terms of signaling and computational overhead with STREK compared to *3GPP* Classic handover in *mm-Wa*ve simulations.
5.6 Attack Simulation in STREK environment	Resistance against Replay and MITM attacks	For Initial Full authentication at home, the TLS protocol through full encryption provides resistance from eavesdropping and data tampering. For roaming-fast authentication, Kerberos provides the cross-realm authentication. As the moving mobile UE does not transmit the password for re-authentication, there is no way for adversarial replay, eavesdropping, tampering, or session hijacking attacks and thus, the STREK scheme is proven to be secure against any network-centric attack vectors.

research are (1) Demonstration of an SDN architecture and framework for overall dynamic control and efficient dataplane programmability through API to the Multimedia IoT/5G applications. (2) A lightweight hybrid cipher scheme for communication channel security and data confidentiality in digital network environment. (3) Exploiting the NFV service-chain and application-awareness in dataplane switches for Co-ordinated Slicing to achieve Quality-of-Experience in live multimedia applications. (4) Fast authentication for handover in low-latency and high mobility scenarios in emerging 5G wireless networks.

The experiments and results make a convincing case that Cloud/Mobile Network Operators (MNO), Content Delivery Networks (CDN) and multimedia content service providers can potentially benefit from integrating lightweight hybrid cipher schemes in SDN. Further, the practical case studies in 4G LTE, IoT, and 5G networks, such as HTTP adaptive streaming, video-slicing applications, and under various attack simulations prove the benefits of SDN. We also address some key requirements for delay-sensitive real-time multimedia applications and attempt to solve major challenges such as lightweight authentication and data protection, handover, and mobility in 5G networks. SDNFV paradigm will greatly transform the existing static nature of the Multi-Access Edge Computing to emerging network architectures in 5G and beyond.

REFERENCES

[1] C. Singhal and Swades De. 2016. Energy-Efficient and QoE-Aware: TV broadcast in next-generation heterogeneous networks. *IEEE Commun. Mag.* 2016, 54 (2016), 142–150.

[2] Cisco. 2020. Cisco VNI Forecast and Methodology, 2015–2020. http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf.

[3] Merly Annie Philip, V. Vaithiyanathan, and Kurunandan Jain. 2018. Implementation analysis of rectangle cipher and its variant. In *Proceedings of the 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT'18).*

[4] J. M. Batalla et al. 2017. Efficient media streaming with collaborative terminals for the smart city environment. *IEEE Commun. Mag.* 2017, 55 (2017), 98–104.

[5] Y. Jin and Y. Wen. 2017. When cloud media meets network function virtualization: Challenges and applications. *IEEE Multimed.* 24, 3 (2017).

[6] S. Rizou et al. 2018. A service platform architecture enabling programmable edge-to-cloud virtualization for the 5G media industry. *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting.* 1–6.

[7] S. A. Alvi, B. Afzal, G. A. Shah, L. Atzori, and W. Mahmood. 2015. Internet of multimedia things: Vision and challenges. *Ad Hoc Netw* 33 (2015), 87–111

[8] ETSI. Mobile Edge Computing (MEC); Framework and Reference Architecture. ETSIGSMEC003V1.1.1 (2016-03). Retrieved from https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/01.01.01_60/gs_MEC003v010101p.pdf.

[9] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. 2008. OpenFlow: Enabling Innovation in campus networks. *ACM SIGCOMM Comput. Commun. Rev.* 38, 2 (2008).

[10] Dongfeng Fang, Yi Qian, and Rose Qingyang Hu: Security for 5G Mobile Wireless Networks. *IEEE Access Spec. Sect. on Trust. Comput.* Retrieved from 10.1109/ACCESS.2017.2779146.

[11] M. N. Asghar, M. Fleury, and S. Makki. 2017. Interoperable conditional access with video selective encryption for portable devices. *Multimed. Tools Applic.* 76, 11 (2017), 13139–13152.

[12] Y. Chen, H. Jia, K. Huang, J. Lan, and X. Yan. 2016. A secure network coding based on broadcast encryption in SDN. *Math. Prob. Eng.* 2016, 7145138 (2016).

[13] F. Ongaro, E. Cerqueira, L. Foschini, A. Corradi, and M. Gerla. 2015. Enhancing the quality level support for real-time multimedia applications in software-defined networks. In *Proceedings of the International Conference on Computing, Networking and Communications (ICNC'15).* 505–509.

[14] Olatunde Awobuluyi, James Nightingale, Qi Wang, and Jose M. Alcaraz-Calero. 2015. Video quality in 5G networks context-aware QoE management in the SDN control plane. In *Proceedings of the IEEE International Conference on Computer and Information Technology.* 1657–1662

[15] Pengcheng Liu et al. 2018. Secure video streaming with lightweight cipher PRESENT in an SDN testbed. *Comput. Mater. Contin.* 57, 3 (2018), 353–363. DOI: 10.32604/cmc.2018.04142

[16] Hassan Noural et al. 2018. One round cipher algorithm for multimedia IoT devices. *Multimed. Tools Applic.* DOI: https://doi.org/10.1007/s11042-018-5660-y

[17] Federico Alvarez et al. 2019. An edge-to-cloud virtualized multimedia service platform for 5G networks. *IEEE Trans. Broadcast.* 65, 2 (2019).

[18] Teerawut Banchuen, Kiattikun Kawila, and Kultida Rojviboonchai. 2018. An SDN framework for video conference in inter-domain network. In *Proceedings of the International Conference on Advanced Communications Technology (ICACT'20).*

[19] Ling Xing, Qiang Ma, Honghai Wu, and Ping Xie. 2018. General multimedia trust authentication framework for 5G networks. *Wirel. Commun. Mob. Comput.* 8974802 (2018). DOI: https://doi.org/10.1155/2018/8974802

[20] Sufyan Almajali, Dhiah el Diehn I. Abou-Tair, Haythem Bany Salameh, et al. 2019. A distributed multi-layer MEC-cloud architecture for processing large scale IoT-based multimedia applications. *Multimed. Tools Applic.* 78 (2019), 24617–24638. DOI: https://doi.org/10.1007/s11042-018-7049-3

[21] Xiaoyu Duan and Xianbin Wang. 2016. Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer. In *Proceedings of the IEEE Communication and Information Systems Security Symposium.*

[22] Subhan Ullah, Lucio Marcenaro, and Bernhard Rinner. 2019. Secure smart cameras by aggregate-signcryption with decryption fairness for multi-receiver IoT applications, *Sensors* 19 (2019), 327.

[23] Ihsan Mert Ozcelik and Cem Ersoy. 2019. Chunk duration–aware SDN-assisted DASH. *ACM Trans. Multimed. Comput. Commun. Applic.* 15, 3 (2019).

[24] Prabhakar Krishnan, Karthik Raghunath, and Krishnashree Achuthan. 2018. Managing network functions in stateful application aware SDN. In *Proceedings of the 6th International Symposium on Security in Computing and Communications.*

[25] Prabhakar Krishnan, Jisha S. Najeem, and Krishnashree Achuthan. 2017. SDN framework for securing IoT networks. In *Proceedings of the International Conference on Ubiquitous Communications and Network Computing*. Springer, Cham, 116–129.

[26] Shuai Zhao et al. 2018. Smooth streaming with MPEG-DASH using SDN-based application-aware networking. In *Proceedings of the Workshop on Computing, Networking and Communications.*

[27] Ugur Acar et al. 2018. Programming tools for rapid NFV-based media application development in 5G networks. In *Proceedings of the IEEE Conference on Network Function Virtualization/Software Defined Networks.*

[28] Charalampos Manifavas, George Hatzivasilis, Konstantinos Fysarakis, and Konstantinos Rantos. 2014. Lightweight cryptography for embedded systems—A comparative analysis. In *Data Privacy Management and Autonomous Spontaneous Security.* Springer, Berlin, 333–349.

[29] A. Biryukov and L. Perrin. 2017. State of the art in lightweight symmetric cryptography. *IACR Cryptology ePrint Archive.* Retrieved from https://eprint.iacr.org/2017/511.pdf.

[30] George Hatzivasilis, Konstantinos Fysarakis, Ioannis Papaefstathiou, and Charalampos Manifavas. 2018. A review of lightweight block ciphers. *J. Cryptog. Eng.* 8 (2018), 141–184. DOI: https://doi.org/10.1007/s13389-017-0160-y

[31] Navid Nikaein, Mahesh K. Marina, Saravana Manickam, Alex Dawson, Raymond Knopp, and Christian Bonnet. 2014. OpenAirInterface: A flexible platform for 5G research. *SIGCOMM Comput. Commun. Rev.* 44, 5 (October 2014), 33–38. DOI: https://doi.org/10.1145/2677046.2677053

[32] Muhammad Reza Z'aba et al. 2014. I-PRESENT: An involutive lightweight block cipher. *J. Inf. Sec.* 5 (2014), 114–122.

[33] Z. Gong, S. Nikova, and Y. W. Law. 2011. KLEIN—A new family of lightweight block ciphers. *RFID. Security and Privacy (Lecture Notes in Computer Science, Vol. 7055).* Springer-Verlag, Berlin, 1–18.

[34] WenTao Zhang, ZhenZhen Bao, DongDai Lin, et al. 2015. RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms. *Sci. China Inf. Sci.* 58 (2015), 1–15. DOI: https://doi.org/10.1007/s11432-015-5459-7

[35] Elena Dubrova and Martin Hell. 2017. Espresso: A stream cipher for 5G wireless communication systems. *Cryptog. Commun.* 9, 2 (2017), 273–289.

[36] J. Daemen and V. Rijmen. 2002. *The Design of Rijndael, AES—The advanced Encryption Standard.* Springer-Verlag, Berlin.

[37] C. Blondeau and K. Nyberg. 2013. New links between differential and linear cryptanalysis. In *Advances in Cryptology—EUROCRYPT 2013*, T. Johansson and P. Q. Nguyen (Eds.). EUROCRYPT 2013. Lecture Notes in Computer Science, Vol. 7881. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-38348-9_24

[38] A. Bogdanov and K. Shibutani. 2012. Generalized Feistel networks revisited. *Des., Codes Cryptog.* 66 (2012), 75–97.

[39] F. Chabaud and S. Vaudenay. 1995. Links between differential and linear cryptanalysis. In *Advances in Cryptology—EUROCRYPT'94.* A. De Santis (Ed.). EUROCRYPT 1994. Lecture Notes in Computer Science, Vol. 950. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/BFb0053450

[40] P. Shantharama et al. 2018. LayBack: SDN management of MEC for network access services and radio resource sharing. *IEEE Access.* DOI: https://doi.org/10.1109/ACCESS.2018.2873984

[41] J. Son and R. Buyya. 2019. Latency-aware virtualized network function provisioning for distributed edge clouds. *J. Syst. Softw.* 152 (2019), 24–31.

[42] Prabhakar Krishnan, Subhasri Duttagupta, and Krishnashree Achuthan. 2019. SDNFV based threat monitoring and security framework for multi-access edge computing infrastructure. *Mobile. Netw. Appl.* 24 (2019), 1896–1923. DOI: https://doi.org/10.1007/s11036-019-01389-2

[43] Prabhakar Krishnan et al. 2019. VARMAN: Multi-plane security framework for software defined networks. *Comput. Commun.* DOI: 10.1016/j.comcom.2019.09.014

Received September 2019; revised November 2019; accepted December 2019