Volume: 14 Issue: 06 Pages: 5705 - 5716 (2023) ISSN: 0975-0290

Performance Study on 5G - NSA Backhaul Network Secured with HIP

Chathurika Weliwita
Department of Computer Science, The Open University of Sri Lanka, Nawala, Sri Lanka
Email: cswel@ou.ac.lk

----------ABSTRACT----------

Fifth generation Non-Stand Alone (5G-NSA) mode offers users an earlier 5G experience before worldwide Stand Alone 5G implementation (5G-SA). In 5G-NSA, operators utilize the existing fourth-generation (4G) networks to provide pre-5G services. In some 5G-NSA deployments, the 4G backhaul network connects the 5G core (5GC) or 4G evolved packet core (EPC) to the 5G new radio (5G NR) network. Nevertheless, implementing security in all network segments is essential to assure end-to-end security in 5G-NSA implementations. Operators must use Internet Protocol security (IPsec) to secure user plane transmissions through 4G backhaul. Host Identity Protocol (HIP) is an alternative method to implement IPsec without disturbing radio or core network protocols to provide node authentication, data encryption with integrity protection, and replay protection to the user plane. This study evaluates the effectiveness of the secure HIP-4G backhaul network to assure end-to-end security in 5G-NSA. According to the results, HIP implementation does not delay message transmissions. Only a slight delay occurs at the security session establishment phase in the HIP Base Exchange process. Hence the HIP implemented 4G backhaul is appropriate to assure end-to-end security in 5G-NSA until the 5G-SA internetworking solutions are implemented.

Keywords - **5G, 5G-NSA, 4G-LTE, Backhaul network security, Host Identity Protocol.**

Date of Submission: March 01, 2023 Date of Acceptance: April 20, 2023

1. INTRODUCTION

Mobile communication network enhancements create a digital transformation that affects all types of industries and changes the lives of everyone. When shifting to fifth-generation (5G) mobile communication networks, the service providers focus on providing 5G services instantly along with enhanced 4G networks [1].

5G focuses on services like Virtual Reality (VR), Augmented Reality (AR), Vehicle to Everything (V2x), and the Internet of Things (IoT), which require even lesser latencies and faster data speeds [2]. With new service requirements in 5G, the service providers need to upgrade their radio, core, and interconnecting networks. This improvement costs much engineering planning and infrastructure implementation [3]. Moreover, the 4G services are required to facilitate the 4G customers before the complete 5G migration. The cost of 5G migration and retaining 4G is only partially viable for service providers. Also, this hurdle may decelerate the 5G migration process.

Two deployment modes are recommended for 5G deployments: Non-Stand-Alone (NSA) and Standalone (SA). In the NSA mode, the 5G services are provided with the aid of 4G networks [4]. NSA mode is practiced globally, and not all 5G deployments are SA [5] [4].

The 5G-NSA standard was finalized in 2017 [6]. The 5G network services are provided using the existing 4G RAN and core network with the addition of a 5G component carrier. NSA amounts to a hybrid methodology of delivering a portion of what 5G offers and uses dual connectivity and spectrum sharing. It provides 5G NR coverage, subject to legacy conditions in the "old" core [4]. NSA increases bandwidth by millimeter wave frequencies [6].

However, the 5G-SA mode implements the 5G Core network and full deployment of all 5G hardware, features, and functionality [6]. The 5G NRs are connected to a 5G Core Network by replacing the current Evolved Packer Core (EPC) and then provide end-to-end 5G performance, including Network Slicing, QoS framework, UltraLow Latency (urLLC), and mMTC [5].

Implementation of 5GC will need more effort, time, and funds; hence the 5G-NSA is the initial choice of the service providers to deliver 5G services to 5G customers [3]. 5G-NSA deployment can be in different modes using distinct sub-networks of the 4G network. For example, the 3GPP (3rd Generation Partnership Project) has recommended seven approaches to deploy 5G-NSA.

The immediate launch of 5G was the primary intention of 5G-NSA. However, there are many other reasons for the service providers to start with 5G in NSA mode. One main advantage is the ability to reuse the 4G network while maintaining the 4G services. The service providers

Volume: 14 Issue: 06 Pages: 5705 - 5716 (2023) ISSN: 0975-0290

are also allowed to support 4G coverage gaps. Operators who implement 5G through 5G-NSA will gain a competitive advantage with publicity for customer base expansion and the ability to leverage existing network investments in transport and mobile core [3]. Also, they perceive 5G NSA as an opportunity to improve 5G services in pre-5G deployment to test 5G user devices [7]. At the same time, with 5G NAS, operators receive ample time window to develop 5GC and connect networks [8]. 5G-NSA accelerates 5G NR deployments while 5G Core and x-haul networks are steadily upgraded [4].

In 5G-NSA, the 5G NRs are primarily connected to existing 4G EPC, providing 5G services to end users, including humans and machines. 5G-NSA deployments use the 4G EPC or 5GC network connected to 5G NR via the 4G backhaul network, while 5G x-haul is developed [9]. Hence the initial 5G services are facilitated by the 4G backhaul network. There are two varieties of backhaul networks, wired backhauls use fiber connections, and wireless backhaul solutions employ microwave and mmWave links. Wireless backhaul is commonly used to connect the radio access network (RAN) to the core network when fiberoptics are unavailable, rapid deployments are required, and cost-efficient solutions are necessary.

The backhaul network consists of links from the core network to subnetworks and must be secured to protect the user and organization data and communication. Lack of security could cause large scandals and mistrust, ultimately deterring customers from using the solution [10]. 5G security architecture inherits the 4G security features with different strata and domains [11][12]. With its increasing scale, the current centralized security model is untenable in 5G networks. Hence security functions in 5G are designed to decentralize and handle locally by the processing elements in the network. However, 5G-NSA and 4G networks share security mechanisms [12].

End-to-end security of the 5G-NSA deployment scenario must be achieved by implementing security in each network segment. Cryptographic protection in a 4G backhaul network is mandatory to ensure safety in 5G-NSA communication. From 4G, Radio Network Controller (RNC) is excluded from network architectures, and RNC functions are delegated to evolved node-B (eNodeB/eNB) or next-generation eNB (ng-eNB) and EPC nodes [12]. In practice, to keep network efficiency, the radio network encryption for user data ends at eNodeB. Thus, the data from the radio network to the secure core network is transmitted as plaintext via the backhaul domain, creating a vulnerability in the backhaul network [12]. This unsecured communication segment infringes the mandatory end-to-end security assurance in 4G and 5G-NSA.

Only external security measures are needed if the backhaul nodes are not in a trusted domain/secured environment [13] [11]. However, the definition of trust and physical security for backhaul nodes depends on the network operator's perception of security. When 5G NR is plugged into 4G EPC and coexists with 4G radios as part of the existing network, the additional nodes created by edge computing complicate the security design of the 4G backhaul network. Different denotations on IPsec are employed in 4G backhaul, leading to numerous IPsec deployments in 4G backhaul networks [15] [14]. Other than direct implementations of IPsec, different mechanisms are used to protect the 4G backhaul network. One such protocol is Host Identity Protocol (HIP).

Backhaul network security enhancement using Host Identity Protocol [16] can provide end-node authentication, data encryption, integrity, and replay protection. This architecture implements HIP only at eNodeBs and Security Gateway (SeGW) by inserting HIP as a new layer in the 4G backhaul protocol stack between the transport and network layer. End-Nodes are authenticated in the HIP Base Exchange process. HIP creates security associations between two end nodes, and packets are routed as Encapsulated Security Payload - Bounded End to End Tunnel (ESP-BEET) packets in a connectionless manner using these security associations [8]. This network architecture comprises one or more SeGWs at the interface of the EPC and backhaul network for HIP packet processing before transmitting ESP packets to relevant EPC nodes. SeGW reduces the extra processing from the core network nodes and eliminates direct access to core network nodes. This standalone mechanism will protect 5G communication from 4G EPC or 5GC to 5G RN through a 4G backhaul network without disturbing the core network and radio network architectures.

Performance evaluation of the HIP-implemented 4G backhaul network to understand the performance impact of HIP in a 4G backhaul network used in 5G NSA mode is presented in this paper. A simulated HIP- 4G backhaul network and a standard backhaul network as the control were used in this study. In section 3, the method is described. In the second section, the background of the study is presented. Section 4 explains the results, section 5 discussion, and Section 6 concludes the paper.

2. BACKGROUND

The mobile network in each standard has significant differences, which cause the networks to be substituted completely [17] with the latest standards. With increased demand, the 5G mobile communication standard is getting priority over other mobile communications standards.

In 5G, it is not only about personal communication and information sharing. 5G is expanding into new industries by introducing boundless extreme reality (XR) facilities, seamless IoT capabilities, new enterprise applications, local interactive content, and instant cloud access [18]. Moreover, the 5G networks provide infrastructure for

Volume: 14 Issue: 06 Pages: 5705 - 5716 (2023) ISSN: 0975-0290

delegation, automation, and connectivity to machines and robots [3]. 5G is designed to provide mission-critical services and massive IoT [18] with ten times more wireless capacity [19].

However, 5G migration is a multi-phased process with many considerations when it evolves from 4G to 5G. [10]. More than a simple upgrade of the mobile network will be required when a new spectrum is added and enhance the capacity or use of advanced radio technology. Hence, it must upgrade from the system and architecture levels to the physical layer [20]. The 5G standalone infrastructure deployment will need a global movement. However, the development speed differs geographically due to varied challenges.

Though 5G is not all about improved services over 4G, [18] and 5G is not reflected as a direct replacement for 4G [17], like other legacy standards were replaced by the most recent technology. Both 4G and 5G networks will work concurrently, focusing on providing good speeds on mobile devices all over [17] until the comprehensive 5G-NA coverage one day. Even though mobile service providers are working on providing 5G services to their enthusiastic customers, they must continue improving the 4G network for required services [17]. 5G phase 1 was commenced in 2017 to support these requirements, and the first deployments of 5G are mostly 4G service dependent [4]. Since 5G systems do not require any specific access type or radio technology, there can be 5G deployments using the 4G RAN to access the 5G Core network [3] or 5G NR to access 4G EPC. In the early 5G use cases, mobile service providers considered better internet connectivity the leading service compared to 4G [3].

5G orthogonal frequency-division multiplexing (OFDM) operates based on the same mobile networking principles as 4G with much more flexibility and scalability [18]. When moving from 4G to 5G, MSPs follow approaches where they can utilize the existing 4G network by managing similarities and differences. These approaches would help the MSPs to benefit from cost-effective, marketable, efficient mechanisms to provide highly demanded 5G services [7]. The upgrade from 4G to 5G will occur in stages with good end-to-end planning, financial and engineering costs, and ultimately deploy independent 5G networks [2] [21].

2.1 5G-NSA with 4G

The 5G networks will coexist with 4G networks for some time [22]. The complete 5G performance spread will take multiple years, and the start and end points will depend on the operators based on different business requirements [5][9]. Stepwise implementation would balance investment, new revenue streams, and competitiveness to match their business and technology priorities [23].

The dual mode 5G will benefit the operators to introduce 5G more quickly while preserving the existing services with control of 5G migration [4] [22]. It would allow the service providers to use easy and quick mechanisms to introduce new functionality and maintain updates to increase performance using 5G developments in cloud-native design, network slicing, and Edge deployments [22].

Finally, a gradual transformation from 5G-NSA to 5G SA mode architecture options would occur [6]. The Mobile Service Providers have declared the commercially available 5G SA services [5]. With NSA mode, the operators can provide 5G services to the customers with less cost and overall effort. It is a better rollout option for the service providers while keeping the existing services [4]. Successful coexistence with 4G while 5G growth will reduce risk and best use the current system [23]. Careful planning and implementation will make NSA to SA transition seamless for the user base [6].

With the NR specifications, the service providers can test their wireless performances and standard compliance, perform Radio Frequency (RF) modeling and planning, and then physically deploy the NR [4]. First, these NRs are connected to existing 4G EPC to provide 5G performance in eMBB use cases which will consume almost 75% of all traffic via wireless by 2025 [4]. Nevertheless, in wired access still, only the 4G services are available [4]. The NSA has accelerated 5G deployment with 5G NR and given time for the 5G Core and xHaul developments [11]. 5G-NSA does not support other 5G services like network slicing, 5G QoS framework, or offer ultra-low latency and is mostly like 4G until the 5G core is updated [4][5].

The 5G-NSA architecture will use 5G and 4G network elements to deliver 5G services while providing 4G legacy services. In this approach, the 4G and 5G network segments must be planned carefully to keep the smooth functioning of both services. Hence, the network service providers can plan and design their networks according to user demand, requirements, cost efficiency, low maintenance, and implementation. The reusable components will be maintained while additional 5G features are added to 5GC and 5G RAN. The Backhaul segment is probably the first to replace to handle 5G traffic while other network domains gradually develop [21]. In some network architecture, the backhaul network will be kept as a reusable component. 5G phase 1 and 2 standards mainly focused on the 5G-NSA services [4].

2.2 Backhaul Network

The backhaul network is the transport network segment used by mobile service providers to connect RAN and Core networks. With the addition of users to the 5G network and the proliferation of small cells, the backhaul will have to handle massive traffic [23].

Volume: 14 Issue: 06 Pages: 5705 - 5716 (2023) ISSN: 0975-0290

5G uses a unique internetworking solution. The 5G backhaul will combine wired and wireless based on the deployment area and user traffic. 5G network uses the front-haul to connect radio units to baseband units, and the mid-haul connects distributed units to centralized units. The backhaul, on the other hand, connects baseband units to the 5GC. 5G backhaul, which delivers new 5G eMMB services are same as 4G backhaul with more traffic [4].

4G backhaul network connects eNodeBs to the core network, consisting of an access and aggregation domain. 3GPP specifications and other supplementary specifications from Internet Engineering Task Force (IETF), International Telecommunication Union (ITU) specify the technical requirements for a 4G backhaul network [24].

Besides the physical network, two logical interfaces S1 for inter eNodeB communication and X2 to support the handover process when the user terminal moves from one eNodeB to another, are also included in the backhaul network. S1 traffic is from eNodeB to EPC. In the backhaul, S1 user plane traffic is predominant over other traffic [11]. Backhaul traffic consists of S1 User plane traffic + S1 Control plane traffic + X2 User plane traffic + X2 Control plane traffic + OA and Management Synchronization + Transport protocol overhead + IPsec overhead (optional) [11].

2.3 Backhaul Network Security and Vulnerability.

5G Security procedures between User Equipment (UE) and 5G network functions [23] state that when the UE can connect to 5GC and EPC using an ng-eNB connected to EPC and 5GC, both can select either EPC or 5GC. When the UE selects EPC, the communication will adhere to 4G security [22]. If the UE connects to 5GC, the transmission will apply 5G security specifications [23]. Also, the actions taken by the home network to link authentication confirmation are after the operator's policy and are not standardized [23]. However, guidance to help avoid the proliferation of different solutions is given for the operators to follow.

Current network security models rely on a minimum amount of responsibility distribution with a central point of control and authority for monitoring and tasking [26]. This model is not practical for 5G networks with increasing scales. Hence the security functions will have to be distributed throughout the network and handle issues locally within the processing elements.

In 5G-NSA, the backhaul network connection must be secured to protect the user and organization's data and communication. The 5G-NSA and 4G networks share the exact security mechanisms, whereas the 5G SA network supports more security features designed for 5G. In the initial implementations of 5G-NSA, the service providers depend on 4G security standards.

The 4G security model briefly describes a secure core and radio network with a vulnerable backhaul network (radio nodes and connections). 4G architecture comprises security concerns due to its flat nature (because RAN protection terminates at eNodeBs). Some design considerations include allowing eNodeB placement in untrusted locations, new business environments with less trusted networks, and keeping security breaches as local as possible [27]. Decentralized security application expects the network elements to resolve security issues within the devices in the 5G network. However, it is impossible to expect physical security in many end nodes.

Generally, in legacy networks, the RNC is placed between the radio network and the core network in the regional center, where physical security is also assured. However, in 4G networks, the RNC functionality is delegated to eNodeBs and EPC nodes. Hence the radio communication (secured by radio protocols) terminates at eNodeB or extends to core network nodes. For network efficiency, radio signals are terminated at eNodeB and discontinue secured (encrypted and authenticated) radio networks [27].

According to 4G backhaul network security specifications, especially 3GPP TS 33.401 [22], the control plane data (S1-C / S1-MME and X2-C / X2-AS) through the backhaul network are protected by Non-Access Stratum (NAS) security. Still, user data (S1-U and X2-U) is covered if backhaul end nodes are protected or trusted.

The definition of trust leads to many interpretations of backhaul data security. One possible denotation provided by NGMN on trust (and un-trust) is based on the physical site security of the node and the ownership of the network [11]. Instead, the trust in a network may depend on other parameters such as network operation management of a single administrative authority, the degree of security an operator wants to reach, assessment of the cost to reach that level of security, and MSPs' attitude on security [15]. Hence the impression of trust depends mostly on MSPs' conception of security. When implemented with 5G-NSA with massive end nodes existing in open spaces, there are better solutions than physical security to achieve backhaul security [26].

Design considerations in 4G networks consist of a significant security vulnerability that never existed in legacy networks, according to 3GPP [25][26]. When blending with 5G-NSA, extra vulnerabilities are exposed in the 4G backhaul network. However, 5G requires additional security. 5G will experience increases in the total amount of data at eMBB, the number of connections in IoT, a requirement for low latency communications [26]. These expansions will limit the capability to inspect network traffic. Vulnerabilities in the 4G backhaul network can be intensified with unencrypted data and unauthenticated end nodes in the backhaul network.

Volume: 14 Issue: 06 Pages: 5705 - 5716 (2023) ISSN: 0975-0290

2.4 4G Backhaul Security Implementations

3GPP has recommended implementing IPsec with IKEv2 (/v1) to protect user plane traffic between eNodeB (cell site) to core-network in S1-U and X2-U interfaces if the eNodeB is in an untrusted domain [7]. IPsec provides data encryption and integrity protection, and IKE authenticates the nodes. The model consists of an IPsec tunnel with ESP-BEET mode transmission tunnels established between eNodeB and core network nodes to carry control (signaling) and data (bearer) traffic. The data through the BEET tunnel is encrypted by ESP protocol at one end and decrypted at the other end [8].

Even though 3GPP proposes IPsec with IKEv2 to implement 4G backhaul security, several practical complications are observed. ENodeB vendors use IPsec and IKEv2 in various concentrations [15]. IPsec applications proposed in [27], [29], and [30] present examples of different partial IPsec implementations. Also, eNodeB vendors commonly use strongSwan (an open-source client software) in varied forms to implement IKEv2 [25]. Most of these deployments do not fully comply with 4G security specifications, such as TS 33.210/401 [11][14].

Other than IPsec, there are additional Security implementations proposed in literature ranging from secured eNodeB hardware [28], secured backhaul architectures [26], and different protocol (ex. HIP) based solutions on subdivisions of 4G networks [26][31].

3. METHOD

3.1 Implementation of HIP

HIP was introduced as a host identification technology to separate an IP address's locator and end-point identifiers. In the Host Identity namespace, the third namespace for the Internet uses a cryptographic identity (e.g., the public key of the asymmetric key pair) to identify hosts and IPs to locate hosts on the Internet. HIP enables continuity of communications across IP address changes by consenting hosts to securely establish and maintain shared IP layer states. The Host Identifiers (HI) are used to create the needed IPsec security associations and authenticate hosts. Transport associations are bonded to HIs (via the HIT or LSI) after HIP decouples the transport from the Internetworking layer. HIP provides a broader approach to securing end-to-end connections.

HIP Base Exchange is a two-party cryptographic process establishing the host communication context, as shown in Fig.1. HIP Base Exchange activated node authentication using their public key as the HI and hashed HI as the HIT. In Base Exchange, sigma-compliant four-packets help to make HIP DoS (Denial of Service) resilient. After a successful Base Exchange, hosts are authenticated, and the ESP transport handling procedure takes place on the data packets using two corresponding HIP associations and four related ESP-SAs [8]. The upper layer protocol packet is wrapped into an ESP header, encrypted, and authenticated in regular transport mode. The resulting ESP packet is subject to IP header processing [8]. After ESP processing and address exchange, the outgoing ESP-BEET mode packet is sent to the network. The outgoing data packet is encrypted (using ESP keys [33] generated by the KEYMAT derived at HIP Base Exchange).

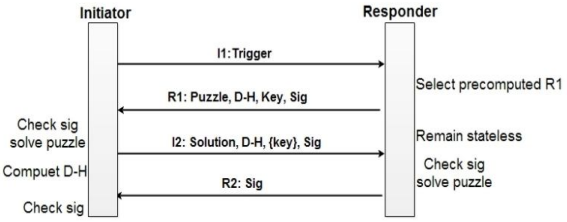

Figure 1: HIP base exchange

The incoming ESP-protected messages are verified and decrypted as in regular transport mode. The resulting clear text packet is subject to IP header processing. In a typical implementation, successful ESP decryption and verification results in a datagram with the associated HITs as source and destination. The datagram is demultiplexed to the right upper-layer socket using HITs instead of IP addresses.

3.2 Implementation of HIP into 5G-NSA Backhaul.

The 5G-NSA deployment modes connect 4G EPC or 5GC with eNB or ng-eNB and utilize the 4G backhaul network. Here the 4G backhaul network implementation with Host Identity Protocol (HIP) is considered [32].

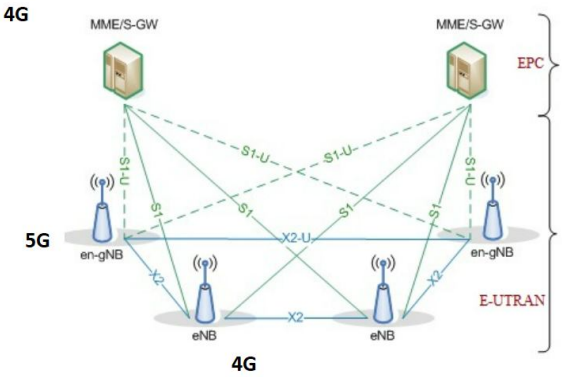

Figure 2: 5G-NSA user plane

In 5G-NSA, the initial implementations utilize a 4G backhaul network by establishing tight internetworking with LTE and 5G NR base stations as in Fig.2. With this, UEs use 4G and 5G connectivity through the secured 4G backhaul and establish end-to-end security for the user plane communication.

Volume: 14 Issue: 06 Pages: 5705 - 5716 (2023) ISSN: 0975-0290

3.2 Performance Evaluation of HIP-4G vs. 4G Backhaul Network.

This study evaluates the HIP-implemented 4G backhaul network against the existing 4G backhaul implementations. Two 4G backhaul networks were designed with the same composite modules as HIP-4G nodes but without the HIP sub-module. The 4G network with the HIP model was compared against the 4G backhaul network to identify the HIP effect on the 4G backhaul network.

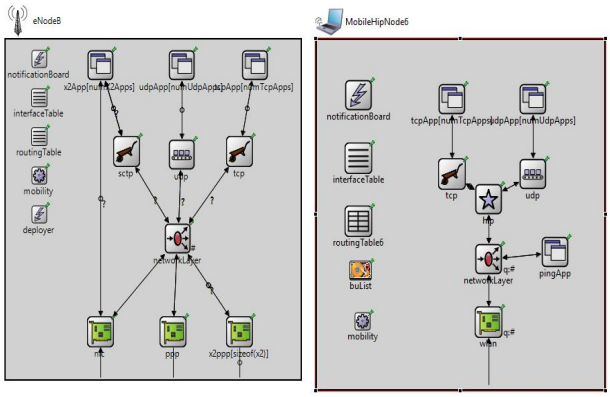

Figure 3: (a) eNodeB used in Simu4G (b) eNodeB used in HIP-4G backhaul network.

This evaluation simulates a 4G backhaul and HIP-4G network in an OMNeT++ event simulator. init-HIPSim++ framework [34] was integrated into the OMNeT++ event simulator [35] with INET [36]. For the simulation of the 4G backhaul network with HIP on OMNeT++, both HIPSim++ and Simu4G [37] frameworks are used.

SimuLTE network nodes are compound modules, while the 4G stack is implemented in the 4G NIC module [17]. 4G NIC was not implemented in nodes used for the simulation model to keep the model simple, and the purpose of the study is to evaluate only the HIP effect on the 4G backhaul network. Other sub-modules are identical to the HIP nodes in HIPSim++, as in Fig.3. Since HIP operates between the transport layer and network (or IP) layers, the underlying NIC (Link and Physical) layer does not directly influence HIP services.

Other than NIC, Application (TCPApp, UDPApp), Transport (TCP, UDP), and Network (IP) layers are common to both frameworks since they are extended from the INET framework. Therefore, simulation model nodes use HIP nodes with few changes to adapt to the proposed architecture. Communication channels use wireless and Ethernet modes. Since HIPSim++ still needs to implement security functionality fully, a performance study on security functions is impossible [37][38].

Mobility may affect HIP functionality. The HIP must maintain HIP associations between sender and receiver at HIP handover procedures, which involve many message transmissions between nodes. Mobile eNodeBs were used to study the mobility effect. Therefore, networks with stationery and mobile eNodeBs were modeled as follows [39][40].

a. HIP-4G backhaul network with Stationary eNodeBs

b. HIP-4G backhaul network with Mobile eNodeBs

c. 4G backhaul network with Stationary eNodeBs

d. 4G backhaul network with Mobile eNodeBs

The following experiments were conducted on the above four networks.

1. Round Trip Time (RTT) vs. sequence for a single TCP packet
2. Average Round Trip Time (RTT) vs. series of TCP packet stream
3. Average TCP throughput for a stream of TCP messages of a mobile eNodeB
4. Average Base Exchange time (Bex duration) for a mobile eNodeB
5. Average Base Exchange time vs. number of eNodeBs (senders)
6. The average percentage of successful Base Exchanges per unit time vs. number of eNodeB attachments and session establishments

4. RESULTS

The results according to each experiment are described in this section.

4.1. Experiment 01: Round Trip Time (RTT) vs. Sequence for Single TCP Packet.

Measure RTT for TCP message transmitted from a sender (eNodeB1) to a receiver (segw1) and echo back to the sender. Time measurements were taken as completion of the following tasks by the TCP message:

- Timeout 1 (tOpen)
- Base Exchange start time
- Base Exchange finish time
- TCP connection establishes time at the sender.
- TCP connection establishes time at the receiver.
- Timeout 2 (tSend)
- Data message transmission time to the receiver
- Echo messages receive time at the sender.

TCPEchoApp response time was set to 0S (Zero Seconds), so it was retransmitted immediately when the receiver received the message. RTT considered in this scenario can be calculated as,

Volume: 14 Issue: 06 Pages: 5705 - 5716 (2023) ISSN: 0975-0290

(4) RTT = Echo msg receive time at sender - Time out 1 – (Time out 2 – TCP connection establish the time at the receiver)

RTT has measured for four (4) different network simulations as mentioned earlier; HIP-4G backhaul with stationary eNodeBs, 4G backhaul with stationary eNodeBs, HIP-4G backhaul with mobile eNodeBs, and 4G backhaul with mobile eNodeBs.

Simulations were executed 20 times with different seeds. Averaged RTT values were used to plot the graphs.

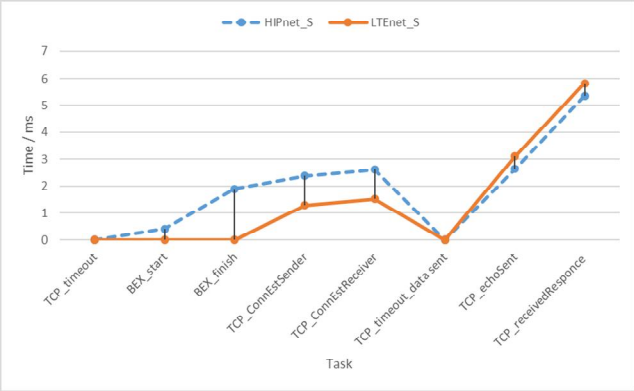

Figure 4: Execution sequence vs. time (stationary eNodeB)

The entire curve in Fig.4 depicts the round-trip time (RTT) of the TCP message. Only connection establishment times differ significantly when a single message flows through the networks. Timeouts were zeroed, and time gaps in mile-seconds (ms) were used to plot.

The time to establish HIP Association and TCP connection in a HIP-4G network is higher than a regular 4G network consumed. That time gap (nearly 1 ms) is because of the HIP Base Exchange process. TCP connection establishment times were considered because the HIP Base Exchange process runs along with the TCP connection establishment process.

When data is sent at the trend, according to Fig.4, the HIP-4G network consumes less time than the 4G network. If RTT is considered the time from connection establishment (tSend) to time echo acknowledgment, the average RTT values for each network can be calculated below.

Average RTT HIPnet_S = 5.3494 ms
Average RTT 4Gnet_S = 5.8204 ms

When TCP throughput is considered as,

(5) TCP throughput = TCP message size / RTT

Average TCP throughput for HIPnet_S = 186936.852731145 bps = 18.7 kbps

Average TCP throughput for 4Gnet_S = 171809.497629207 bps = 17.1 kbps

TCP throughput is increased in the HIP-4G backhaul network because of the HIP association and its transmission mode, i.e., ESP BEET mode.

As the second step of experiment 1, we studied the effect of mobile eNodeB on HIP association aeration and TCP connection establishment processes. Fig.5 presents the average times consumed for each step in the connection establishment process. Considered networks in the figure were HIP_4G mobile network -HIPnet_M and 4G mobile network – 4G_M.

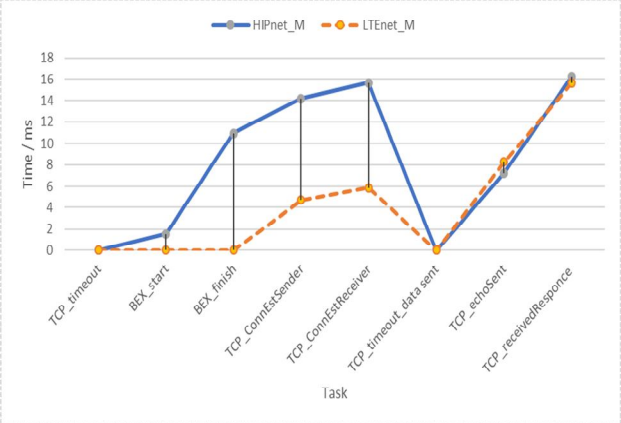

Figure 5: Execution time profile of TCP packet (mobile eNodeB)

According to Fig.5, in the case of mobile eNodeBs TCP connection establishment and HIP association establishment process, the HIP-4G network consumed more time than the 4G network. This time gap was significantly large when compared to stationary models. When the eNodeB moved, HIP's mobility management (Update process) consumed more time. Still, the average time gap is nearly 10ms. In data transmission, HIPnet_M behaves the same as the 4Gnet_M, and average RTT values for each network were:

Average RTT HIPnet_M = 1.619 ms

Average RTT 4Gnet_M = 1.558 ms

Average TCP throughput values were:

Average TCP throughput for HIPnet_M = 61760.7510327196 bps = 61.8kbps

Average TCP throughput for 4Gnet_M = 64163.0453755526 bps = 64.1kbps

Therefore, in the case of mobile HIP eNodeBs, the execution time (RTT) and throughput performance are

Volume: 14 Issue: 06 Pages: 5705 - 5716 (2023) ISSN: 0975-0290

like the 4G network due to the HIP update process with the mobility of the nodes.

4.2. Experiment 02: Average RTT vs. Sequence of TCP Packet stream.

In this experiment, a single TCPSession application sends a sequence of messages.

500B at tSend = 30s
1000B at tSend = 31s
1500B at tSend = 32s

TCPmss (maximum message size) was set to 1024 and receive window to 1000000. As in the first experiment, 20 simulation runs with different seeds were carried out for all four networks, and the durations were collected.

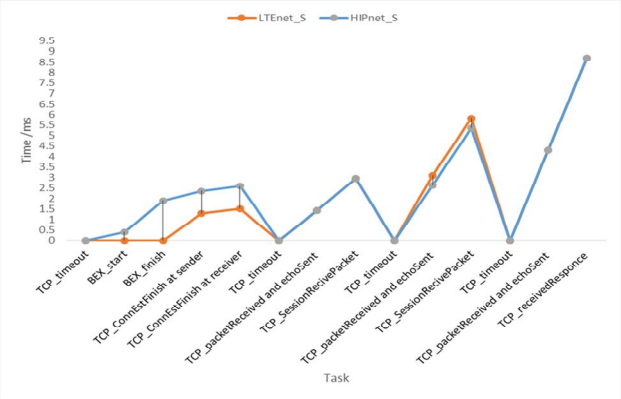

Figure 6: Execution time profile of TCP packet stream when eNodeB is stationary.

The results for stationary eNodeB are shown in Fig.6. In the connection establishment process, only the TCP connection establishment and HIP session establishment have consumed more time. After the connections were established, HIP did not significantly affect the message/data transmission. Furthermore, at the message/data transmission, the RTT value in the HIP-4G network was less compared to the standard 4G network. According to Fig.6, mobile HIP, eNodeB consumes more time in connection establishment and HIP association creation. Also, at data/message sending, the HIP_4G network takes more time than a standard TCP network because of HIP mobility management with the update process.

4.3. Experiment 03: Average TCP Throughput for a Stream of TCP Messages of a Mobile eNodeB

The mobility of an eNodeB can affect Base Exchange time and message transmission time. For a mobile node, more transmissions are involved than in a stationary scenario. The Base Exchange time was measured for 20 different runs with different seeds to study the delay in HIP message exchange when eNodeB is moving.

TCP message size = 1000B
tOpen (t = 25s)
tSend (t = 30s)

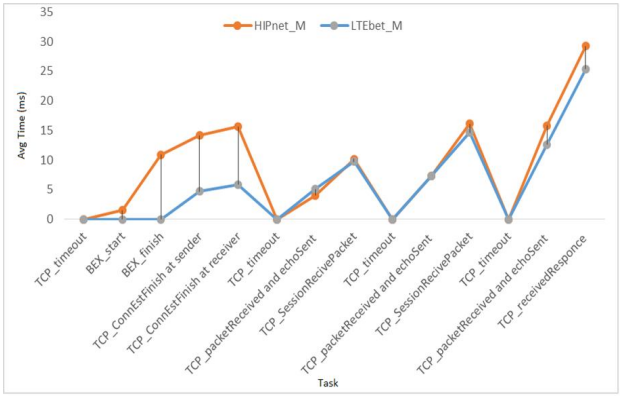

Figure 7: Execution time profile of TCP packet stream when eNodeB is moving.

In this experiment, two networks HIPnet_S and 4Gnet_S, were considered. When TCP data packets were transmitted through the HIP-4G backhaul network, TCP throughput was increased compared to the regular 4G backhaul network. TCP packet size was increased for each run, and TCP throughput was calculated.

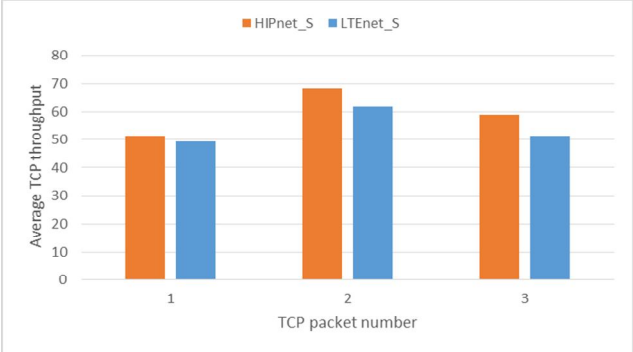

Figure 8: A throughput increase in each message's HIP-4G backhaul network.

4.4. Experiment 04: Average Base Exchange Time (Bex duration) of a Mobile ENodeB.

In this experiment, we studied the Base Exchange time variation when the initiator eNodeB moves. The time consumed to establish connections (Base Exchange time duration/ time taken to establish a HIP association) for the mobile eNodeB was measured. In addition, the Base Exchange start time (BexStart) and finish time (BexFinish) were recorded to identify any effect on Base Exchange start and finish times with the node mobility. The network

Volume: 14 Issue: 06 Pages: 5705 - 5716 (2023) ISSN: 0975-0290

diagram in Fig.9 was simulated (HIP-4G network with mobile eNodeB) for this experiment.

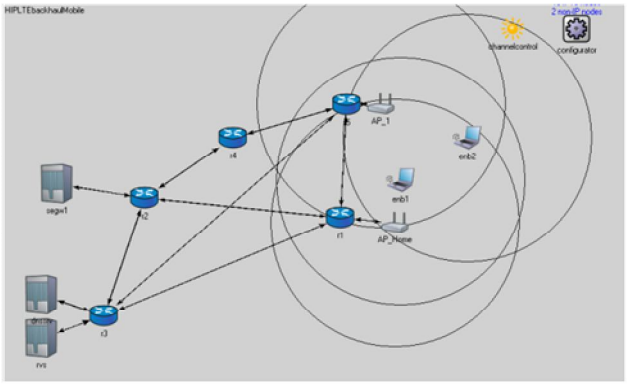

Figure 9: Increasing number of eNodeBs in HIP-4G network.

HIP Base Exchange time was measured when the number of eNodeBs requests for HIP session establishments increased. This experiment was conducted with ten different seeds for HIP -the 4G network. The number of eNodeBs was increased by adding one eNodeB per round for all the eNodeBs.

tOpen = 30s
tSend = 40s
Base Exchange time = Bex Finish time – Bex start time

Figure 10: Base Exchange time for mobile HIP node

When the node is moving, the connection establishment time varies. Even though Base Exchange time goes in mobile HIP eNodeB, as in Fig.10, the maximum Bex time is 11.2 ms (peak value may be because of an impurity). The variation is between 10ms and 8ms other than the first and fifth Bex.

The variation median is 9.19ms. Hence even if the eNodeB is mobile, the Base Exchange time is 2ms for various connection establishments at maximum. Mobile eNodeB takes 9.19 ms to create a HIP association, while stationary eNodeB takes 1.48 ms to establish a HIP association which may be because of mobility management overhead.

4.5. Experiment 05: Average Base Exchange Time vs. Number of ENodeBs (senders).

HIP Base Exchange time was measured when the number of eNodeBs requests for HIP session establishments increased. This experiment was conducted with ten seeds for HIP, the 4G network.

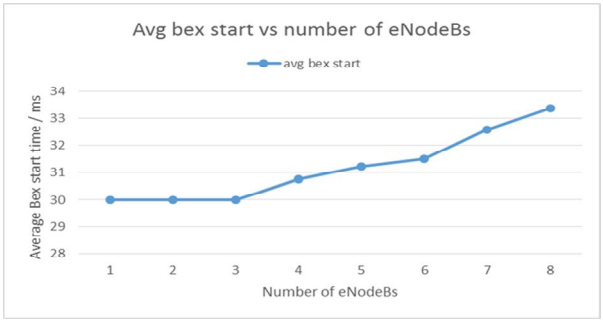

Figure 11: Base Exchange Start time.

The number of eNodeBs was increased by adding one eNodeB per round for all the eNodeBs.

tOpen = 30s
tSend = 40s
Base Exchange time = Bex Finish time – Bex start time

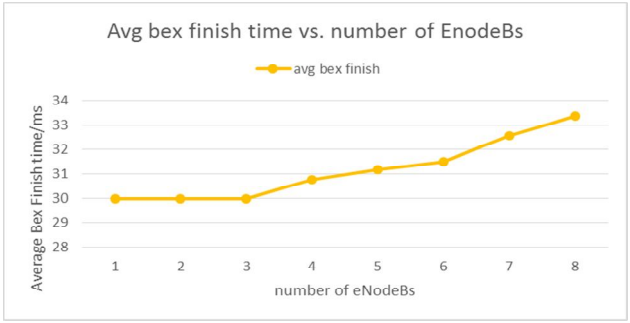

Figure 12: Base Exchange finish time vs. number of eNodeBs

According to Fig.11 and Fig.12, when the number of eNdoeBs is increased, the Base Exchange start time is delayed (Fig.11), in parallel to the start time Base Exchange finish time was also delayed (Fig.12).

4.6. Experiment 06: Average percentage of successful base exchanges per unit time vs. the number of eNodeB attachments and session establishments.

There can be congestion and packet losses when many eNodeBs attempt to make connections and establish HIP associations. This experiment studies the number of complete base exchanges when the number of eNodeBs increases in a unit of time.

Volume: 14 Issue: 06 Pages: 5705 - 5716 (2023) ISSN: 0975-0290

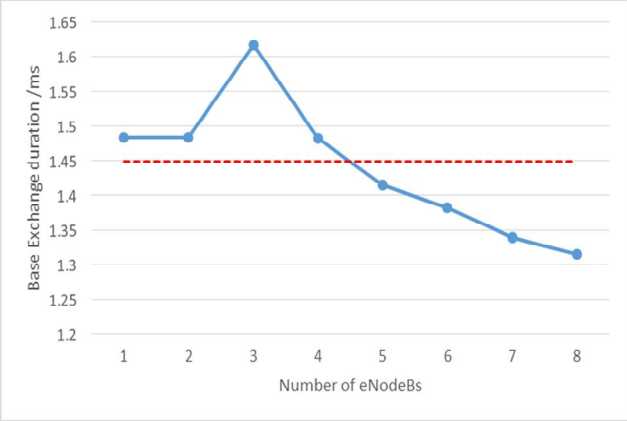

Figure 13: Average Base Exchange time vs. number of eNodeBs

Unit time = 35s
tOpen = 30s
tSend = 40s

Completed Base Exchanges were counted when Bex's finish time was within 35s. Values are averaged for ten runs with different seeds.

.

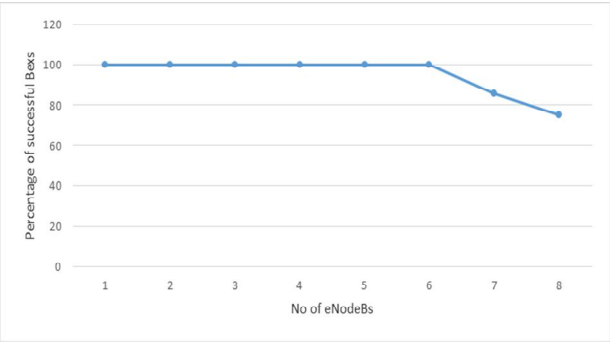

Figure 14: Incomplete Base Exchange percentage vs. number of eNodeBs

According to Fig.14, after a certain number of eNodeBs, the number of completed Base Exchanges decreased. Even though these base exchanges were not met at the measured unit time, packets were not dropped. Base Exchanges were completed at 39s, 9 seconds later. That means the base exchange delay also increases when the number of base exchange requests increases.

5. DISCUSSION

Implementing 5G-NSA using 4G networks utilizes the existing 4G network segments. This study considered reusing a 4G backhaul network with security implementation. In the studied backhaul design, HIP was implemented into the end nodes of the 4G backhaul network. HIP processes the user and control data between the transport and network layers. This processing applied authentication, encryption, and integrity protection to the data transmitted and nodes in the network.

The HIP-4G architecture was validated on its performance to evaluate its capability to perform as a solid solution to 4G backhaul vulnerability. This paper presents the evaluation to understand the HIP effect on the HIP-4G network.

In the performance study, when a HIP-4G backhaul network uses a single connection to transmit a TCP packet, considerable latency was detected only at the connection establishment between two nodes. When a TCP connection is established in the HIP-4G backhaul network, the Base Exchange process is also initiated. HIP association between the nodes is established with ESP security associations (ESP-SAs). After HIP association and ESP-SAs were created, the nodes could send and receive data. At the same time, the throughput of the HIP-4G network manifested a higher throughput than the 4G backhaul without HIP.

This behavior is the same for a mobile eNodeB with additional latency at connection establishment. For the Mobile eNodeB to establish associations, it takes an average of 9.19ms, whereas stationary eNodeB takes a 1.44ms average because of HIP processes for mobility and multihoming.

In the case of TCP message streaming, the behavior was the same, and HIP-4G backhaul illustrated a significant throughput gain in both stationary and mobile states. Messages were sent with increasing average throughput in the HIP-4G backhaul network.

As the scalability of the HIP-4G network was tested with increasing eNodeBs with TCP connections, the Base Exchange start time was delayed, and the duration to complete Base Exchange was decreased. While the number of eNodeBs increased, the number of connections established exponentially reduced to a fixed number. These issues can be solved with load-balancing mechanisms, for example, by using distributed SeGWs. The latter performance evaluations were performed without complete HIP security implementations. If the security algorithms were executed, the average execution times would exceed the presented.

6. CONCLUSION

5G-NSA is the initial implementation mode for 5G. There are many advantages to starting with NSA mode. One is the ability to use the existing 4G network infrastructure to offer 5G services to customers. NSA is a faster way to serve 5G mobile users with less cost and effort. Until the 5GC and 5G internetworking are implemented, the service providers can use 5G NR to elevate the 4G experience to the pre-5 G experience. Different models use the 4G network to offer 5G services.

5G-NSA is deployed in different ways, sometimes, the 4G EPC is used to serve the 5G NRs, and at times 5GC is connected to 5G NRs. Either way, the 4G backhaul to connect the NRs and core networks would be utilized until

Volume: 14 Issue: 06 Pages: 5705 - 5716 (2023) ISSN: 0975-0290

the service providers implement the 5G x-haul networks. When implementing 5G services on top of 4G networks in the 5G-NSA mode, the 4G network segments are reused.

Hence 4G backhaul network is an essential component in 5G-NSA architecture. At the same time, when implementing end-to-end security in the 5G-NSA networks, it is crucial to focus on protecting connecting elements. Usually, the 5G NR is generally secured, and 5GC and 4G EPC are secured. The backhaul network, which connects the secured 5G NRs and 4G RN with 5GC and 4G EPC, is not guaranteed for user plane data. To improve 4G backhaul network security, IPsec is accepted as a solution.

Service providers implement security in 4G backhaul using various IPsec solutions. In this work, a 4G backhaul security solution using HIP was studied. Here HIP is used to secure backhaul without direct IPsec implementation. HIP can provide node authentication, encryption, integrity protection, replay protection, and attack resilience. With these capabilities, HIP can be deployed in backhaul end nodes eNodeBs and SeGW, which limits HIP protocol to the backhaul network.

It is important to have separation from core networks and radio networks for the interconnecting network segment, which is the 4G backhaul network, when segmenting the 5G-NSA network. The HIP implementation limited to 4G backhaul facilitates the separation. When evaluating the impact of HIP on the data transmission performance, the HIP effect is detected mainly at the connection establishment phase, where nodes are authenticated via the Base Exchange process, creating latency. However, during data transmission, HIP-4G can provide high throughput. Since HIP is between layer-2 and layer-3, its implementation does not impact 4G protocols significantly. This architecture can fully comply with 3GPP security requirement standards with additional security.

Notably, the security requirement in the connecting networks is increasing with introducing the 5G NR to the existing networks. The increasing number of users requires fast and low-latency connections, which leads to open and accessible base stations everywhere as a nature of the 5G NR. These ng-eNBs may not be physically protected or impossible to defend concerning their available places. Hence, the service providers must focus on the backhaul network security, and HIP is easy for them to implement IPsec into their backhaul network. The HIP is needed to implement only at end nodes. HIP can be separated from normal operations hence making it easy to implement. With further evaluations of its capabilities and effects, HIP can become the permanent solution for 4G backhaul security.

REFERENCES

[1] “5G Wireless Backhaul | Networks Solutions | Samsung Business Global Networks,” *Samsung global_nw*. https://www.samsung.com/global/business/networks/solutions/wireless-backhaul/ (accessed Jan. 20, 2023).

[2] "5G Deployment Options-Operators to Drift from 4G to 5G," *The 5G Zone*, Dec. 23, 2019. https://the5gzone.com/index.php/5g-deployment-options/ (accessed Jan. 13, 2023).

[3] “A guide to 5G network security," *Ericsson.com*, Sep. 18, 2019. https://www.ericsson.com/en/security/a-guide-to-5g-network-security

[4] L. Badman and T. Nolle, "Enterprise 5G deployment options and how to procure them | TechTarget," *Networking*. https://www.techtarget.com/searchnetworking/tip/Enterprise-5G-deployment-options-and-how-to-procure-them (accessed Jan. 20, 2023).

[5] B. Lavallée, “Spotlight on 4G/5G backhaul networks,” *www.ciena.com*. https://www.ciena.com/insights/articles/spotlight-on-4g-5g-backhaul-networks.html

[6] C. Gartenberg, "5G is almost here — here's how everyone's getting ready," *The Verge*, Sep. 07, 2018. https://www.theverge.com/2018/9/7/17829270/5g-phone-cell-mobile-network-hardware (accessed Feb. 23, 2023).

[7] “Ericsson Mobility Report,” www.ericsson.com, Sep. 07, 2020. https://www.ericsson.com/en/reports-and-papers/mobility-report

[8] P. Jokela, R. Moskowitz, and J. Melen, "Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)," *IETF Datatracker*, Jul. 15, 2015. Accessed: Feb. 10, 2023. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-jokela-hip-rfc5202-bis-00

[9] A. R. Prasad, S. Arumugam, S. B, and A. Zugenmaier, "3GPP 5G Security," *Journal of ICT Standardization*, vol. 6, no. 1, pp. 137–158, 2018, doi: https://doi.org/10.13052/jicts2245-800x.619.

[10] J. Häglund, "How to handle 5G migration successfully," *www.ericsson.com*, Jul. 20, 2018. https://www.ericsson.com/en/blog/2018/7/how-to-handle-5g-migration-successfully (accessed Jan. 03, 2023).

[11] “Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401 version 15.7.0 Release 15).” Available: https://www.etsi.org/deliver/etsi_ts/133400_133499/133401/15.07.00_60/ts_133401v150700p.pdf

[12] “5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.4.0 Release 15)." Accessed: Jan. 10, 2023. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.04.00_60/ts_133501v150400p.pdf

[13] M. Liyanage, P. Kumar, M. Ylianttila, and A. Gurtov, "Novel secure VPN architectures for LTE backhaul networks," *Security and Communication Networks*, vol. 9, no. 10, pp. 1198–1215, Jan. 2016, doi:

Volume: 14 Issue: 06 Pages: 5705 - 5716 (2023) ISSN: 0975-0290

https://doi.org/10.1002/sec.1411.

[14] "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 version 15.1.0 Release 15)," 2018. Accessed: Jan. 23, 2023. [Online]. Available: https://www.etsi.org/deliver/etsi_TS/133200_133299/133210/15.01.00_60/ts_133210v150100p.pdf

[15] P. Donegan, "The Security Vulnerabilities of LTE: Risks for Operators A Heavy Reading Executive Overview," 2013. Accessed: Jan. 20, 2023. [Online]. Available: https://www.juniper.net/assets/us/en/local/pdf/additional-resources/hr-security-vul-lte-wp.pdf

[16] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host Identity Protocol," *www.rfc-editor.org*, Apr. 2008, doi: https://doi.org/10.17487/RFC5201.

[17] https://www.facebook.com/setimerenptah, "5G vs. 4G | Differences in Speed, Latency, and Coverage Explained | Digital Trends," *Digital Trends*, May 2019. https://www.digitaltrends.com/mobile/5g-vs-4g/

[18] "What is 5G | Everything You Need to Know About 5G | 5G FAQ | Qualcomm," *www.qualcomm.com*. https://www.qualcomm.com/5g/what-is-5g/

[19] "Principles of 5G Backhaul," *ACiiST*. https://www.aciist.com/principles-of-5g-backhaul/

[20] M. M. Ahamed and S. Faruque, *5G Backhaul: Requirements, Challenges, and Emerging Technologies*. IntechOpen, 2018. Available: https://www.intechopen.com/chapters/62142

[21] "Backhaul Evolution for 5G," *Cisco*. https://www.cisco.com/c/en/us/solutions/service-provider/industry/telco/backhaul-evolution-for-5g.html#~5g-requirement (accessed Jan. 13, 2023).

[22] "5G Core (5GC) network: Get to the core of 5G," *Ericsson.com*, 2022. https://www.ericsson.com/en/core-network/5g-core

[23] "5G deployment considerations for future networks," *www.ericsson.com*. https://www.ericsson.com/en/reports-and-papers/5g-deployment-considerations (accessed Jan. 20, 2023).

[24] V. GUEANT, "iPerf - The TCP, UDP, and SCTP network bandwidth measurement tool," *Iperf.fr*, 2013. https://iperf.fr/

[25] "Mobile Network Security | 4g and 5G Network Security," *Fortinet*. https://www.fortinet.com/solutions/mobile-carrier/4g-5g-infrastructure-services (accessed Jan. 13, 2023).

[26] "LTE Security for Mobile Service Provider Networks Juniper Provides a Stable and Secure LTE Network that Differentiates MSPs from the Competition," 2013. Accessed: Jan. 20, 2023. [Online]. Available: https://www.juniper.net/content/dam/www/assets/white-papers/us/en/lte-security-for-mobile-service-provider-networks.pdf

[27] "5G White Paper 2," *NGMN*, Jul. 27, 2020. https://www.ngmn.org/publications/5g-white-paper-2.html (accessed Jan. 10, 2023).

[28] "Alcatel-Lucent Mobile Evolution Transport Architecture Enabling the Profitable Evolution to All-IP." Accessed: Feb. 23, 2023. [Online]. Available: http://pexx.net/pdfs/whitepapers/alcatel_lucent/mpr9500/nl_alu-metabrochure_0608.pdf

[29] M. K. Rahmato, "Impacts of IPsec implementation on LTE IP connectivity," Aalto University. School of Electrical Engineering, 2010. Available: http://urn.fi/URN:NBN:fi:aalto-2020122357510

[30] datenfluss, "Guidelines for LTE Backhaul Traffic Estimation," *NGMN*, Aug. 12, 2011. https://www.ngmn.org/publications/guidelines-for-lte-backhaul-traffic-estimation.html (accessed Jan. 23, 2023).

[31] S. Namal, J. Pellikka, and A. Gurtov, "Secure and Multihomed Vehicular Femtocells," May 2012. Accessed: Jan. 20, 2023. [Online]. Available: https://www.cs.helsinki.fi/u/gurtov/papers/femtocell-vtc.pdf

[32] K. C. Amir, "Trusted Hosts in Host Identity Protocol (HIP)," 2012. Available: https://core.ac.uk/download/pdf/38067073.pdf

[33] S. Kent, *IP Encapsulating Security Payload (ESP)*. (2005). Available: https://www.ietf.org/rfc/rfc4303.txt

[34] "HIPSim++," *omnetpp.org*, 2010. https://omnetpp.org/download-items/HIPSim++.html (accessed Jan. 10, 2023).

[35] "INET Framework - Download," *Omnetpp.org*, 2018. https://inet.omnetpp.org/Download.html (accessed Dec. 19, 2019).

[36] G. Nardini, G. Stea, and A. Virdis, "SimuLTE - LTE User Plane Simulation Model for INET," *simulte.com*. https://simulte.com/tutorial-basic.html (accessed Jan. 20, 2023).

[37] L. Bokor, S. Nováczki, L. T. Zeke, and G. Jeney, "Design and evaluation of host identity protocol (HIP) simulation framework for INET/OMNeT++," *Proceedings of the 12th ACM international conference on Modeling, analysis, and simulation of wireless and mobile systems*, Oct. 2009, doi: https://doi.org/10.1145/1641804.1641827.

[38] A. Virdis, G. Nardini, and G. Stea, "Modeling unicast device-to-device communications with simuLTE," *2016 1st International Workshop on Link- and System Level Simulations (IWSLS)*, Jul. 2016, doi: https://doi.org/10.1109/iwsls.2016.7801579.

[39] J. Okwuibe, "Performance evaluation of HIP-based network security solutions," 2015. Available: https://www.semanticscholar.org/paper/Performance-evaluation-of-HIP-based-network-Okwuibe/423d4bacf2c6c652fce0de3d6f9d6c064b147d69

[40] P. Donegan, "IPsec Deployment Strategies for Securing LTE Networks," 2011. Accessed: Jan. 23, 2023. [Online]. Available: http://go.radisys.com/rs/radisys/images/paper-seg-ipsec-deployment.pdf