Jestr

Journal of Engineering Science and Technology Review 11 (1) (2018) 199 - 207

JOURNAL OF
Engineering Science and Technology Review

Research Article

www.jestr.org

On Virtualization and Security-Awareness Performance Analysis in 5G Cellular Networks

Mamdouh Alenezi[1], Khaled Almustafa[2] and Mohamed Hussein[3]

[1]*College of Computer & Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia*
[2]*College of Engineering, Prince Sultan University, Riyadh 11586, Saudi Arabia*
[3]*Western University, London, Ontario, Canada*

Received 18 November 2017; Accepted 7 December 2017

Abstract

Recently, Fifth Generation (5G) cellular networks have gained promise as a paradigm that could provide rich computational resources for users. Virtualization is a key technology for wireless communications, especially in standard Long Term Evolution (LTE) systems, which enable cloud based multi-tenancy business models through providing a shared scalable resource platform for all users. Despite the potential significance of virtualization for cellular networks, several challenges remain to be addressed. For cellular networks, providing multiple levels of security is essential to support different levels in information sensitivity. However, placing different customers' services requirements on a virtualized evolved Node B's (eNB's) scheduler may lead to noticeable security vulnerabilities. In this work, we present an overview of cellular network security issues in a fully virtualized environment along with their preventative measures. Virtualization is implemented by allowing service providers to share their resources while performing different scheduling policies and sharing one eNB. To evaluate the considered framework, the average delays for different traffic types were measured. The results of the simulation showed that virtualization could noticeably reduce average user equipment delay compared with the non-sharing scheme.

Keywords: 5G Cellular Networks, LTE Scheduling, Virtualization, Security-Awareness.

1. Introduction

Wireless networking provides various advantages, particularly improving productivity due to increased accessibility to information resources [1, 2]. However, wireless technology is extremely vulnerable to new threats and exposes the existing profile to additional information security risks [3, 4]. For instance, unencrypted or weakly encrypted algorithms allow attackers to read private information, thereby compromising data confidentiality.

Wireless networks have recently witnessed a tremendous growth in the data traffic due to the increase in the number of users that are always demanding higher data rates [5, 6]. In the Third Generation Partnership Project (3GPP), to cope up with the new demand for increased data traffic, network virtualization based architectures are being proposed for next generation networking in wireless domain [6], especially in Fifth Generation (5G) wireless networks [7]. The sharing of resource blocks (RBs) by services' providers (SPs) has gained significant attention in [6]. Virtualization has helped in delivering number of benefits to operators such as sharing common infrastructure reduces the number of physical components required in the network resulting in minimizing their environmental and financial impact. Virtualization have almost made savings of over 60 billion USD in both operation and expenditures over five years worldwide [8].

The Long Term Evolution (LTE) is designed by incorporating high security measures, by using strong cryptography and mutual authentication mechanisms between all network elements in LTE core [8]. However, in a virtualization deployment, attackers can target mobile user equipment (UE) and LTE core with malware and spam, through eavesdropping, internet protocol (IP)-spoofing, denial-of-service (DoS) attacks, and numerous other cyberattacks [9, 10]. SPs are aiming to use 5G deployment for expected increase business profitability but still have to fix number of security issues [5, 11]. Hence, to protect profit of SPs from being spent on the process of recovery and remediation due to frequent security breaches, SPs should curtail all sorts of security risks in both LTEs and IP, and this is achievable through active investment in preventative security measures.

In the literature, few significant efforts have focused on mobile security challenges with respect to virtualization deployment. First, objective of this paper is to create awareness among the SPs by providing them with relevant information and enabling them to acquire an understanding of the various threats involved in wireless network virtualization based architecture deployment and how to avoid these security problems using preventative measures.

The increased exposure to threats related to the security in LTE networks caused due to open architectures with network elements having multiple interconnections could potentially cause SPs to face financial losses and also could lead to tarnished business reputation. To highlight the active role that SPs could take in securing LTE networks, during

*E-mail address: malenezi@psu.edu.sa
ISSN: 1791-2377 © 2018 Eastern Macedonia and Thrace Institute of Technology. All rights reserved.
doi:10.25103/jestr.111.24

daily operations, and while providing services to its customers, the following sections will review the involved security issues and their measures to prevent and overcome them.

Resource sharing is another key challenge for SP providers. Figure 1 shows how resources are shared among users by SPs and then scheduled by eNB. This paper also compares two most common scheduling algorithms i.e. static and dynamic using detailed simulation and performance analysis and validate effectiveness of virtualized schedulers under security attack.

The remainder of this paper is organized as follows: Section II presents the expected LTE security awareness including security issues and preventative measures, Section III introduces the overview of the system model, Section IV presents our problem formulation, Section V discusses simulation results, and Section VI presents the conclusions.

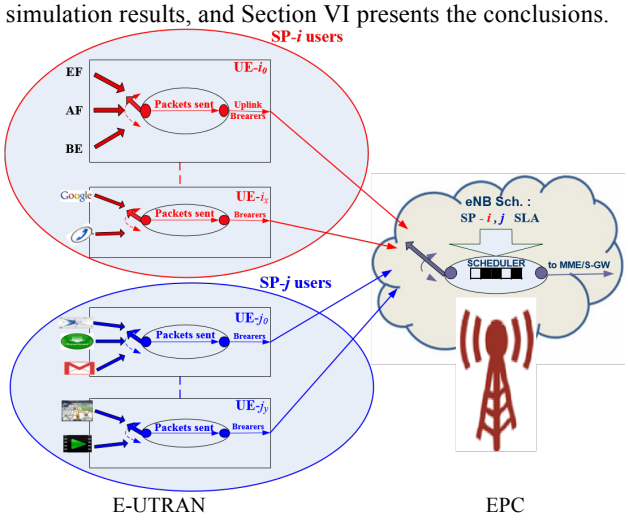


Fig. 1. SPs implementing different scheduler policies and sharing radio RBs in a single eNB.

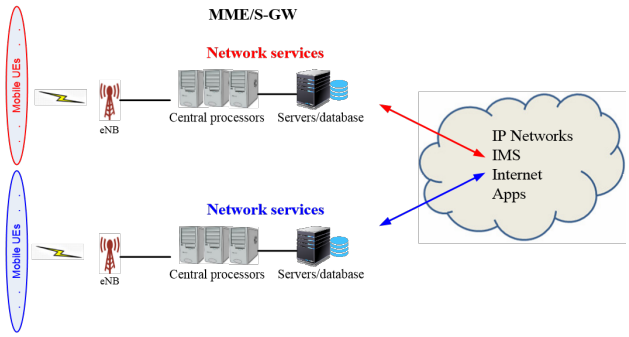


Fig. 2. LTE system architecture.

2. LTE Security Awareness

The security management complexity is considered as key challenge as it is facing the steady rising attackers' interests [12]. In this Section, some of them most common issues that are faced in wireless networks including DoS attack.

2.1. Issues and Preventative Measures

Following are some of the most common security issues and their preventative measures in LTE architecture as shown in Figure 2 that consists of network segments: UE, evolved node B (eNB) access, and evolved packet core (EPC) [13, 14].

1) UEs

UEs are the end communications users that can be exposed to various security issues like:

- Physical Attacks
- Risk due to the loss of data
- Threats at application layer from malware, viruses, and phishing

Physical Attacks: UEs are small, portable, and prone physical theft device itself. These devices can be also tampered making possible to access and attack the operator's networks.

Risk due to the loss of data: New UE are capable of downloading and storing more data than before, thus making them highly vulnerable to the attacks from infiltrators that are related to the data loss on the devices.

Application layer vulnerabilities: The present network architecture is all IP-based, as a result of which all UEs and LTE network elements work with IP packets. This opens up to new issues related to the vulnerabilities in IP-based systems that traditionally related to Internet such as malware, viruses, spam. Proper mechanisms should be in place to protect the integrity of the UE, the overall security in the LTE edge as wells as the subscriber, and finally the overall bandwidth (BW) usage on the SP network [15].

Preventative measures:

- Subscriber Education
- Antivirus Applications
- Strong Authentication

Subscriber Education: It is important to educate the subscribers about the potential damages that could be caused by unsecured resources. It is advised to keep the resources in personal reach and location feature can be turnedoff for improved privacy.

Anti-virus Applications: Attackers are always looking for new ways to attack by making new viruses, malware, spyware or focusing on some vulnerabilities, it is essential the UEs should install and update anti-virus applications regularly [16].

Strong Authentication: Strong authentication mechanisms must be in place before accessing the contents of the UE from outside users. This will prevent attackers from having immediate access to the data on the UEs.

2) eNB Access.

In the LTE network architecture, the eNB is the communication node between the UE and EPC network. It is also the intersection point wherein SPs are sharing their available RBs.

Security Issues:

- Physical attacks
- Rogue eNBs
- Privacy

Physical attacks: with the emergence of smaller eNBs, located in public domains, they are now more vulnerable to physical tampering, through which the SP network can be accessed and compromised.

Rogue eNBs: Rogue eNBs can be installed by the attackers to emulate the operator's node and through them the attackers can intercept the traffic emanating from the UE. The attackers can therefore listen to the traffic and redirect the traffic to the malicious parties [17].

Privacy: Attackers can identify the location of the UE through spurious paging instructions and comparing the

temporary mobile subscriber identity with the permanent international mobile subscriber identity (IMSI). In addition to this the attackers can also respond to the intercepted authentication process, thus enabling them to determine the exact location of the physical device.

Preventative measures:

- Physical security
- Authentication, authorization, and encryption
- Security architecture

Physical security: SPs have to devise mechanisms for physical safety and security of the eNBs placed in public locations, which can be accessed and tampered to expose the SP's network.

Authentication, authorization, encryption: 3GPP specifies access security, which includes authentication, authorization, and traffic safeguard between the UE and EPC networks. Strong level of encryption between the eNB access and UE will identify both rogue eNBs and man in the middle attack. Adopting public key based infrastructure, which stores the public key of the SP in the universal subscriber identity module that allows the UE to be able to encrypt private data such as the IMSI [18].

Security architecture: SPs have to ensure that the service quality is not affected with the inclusion of the security architecture that consumes BW resources for the process of authentication and encryption.

3) Evolved Packet Core

The EPC is the core of the LTE wireless network that will manage security related processes such as authentication, accounting and authorization. In addition to that, it will perform network management functions such as IP address allocation, mobility management, QoS, and control signaling.

Security Issues:

- Unauthorized access
- Over-billing attacks (IP address hijacking/spoofing)

Unauthorized access: Unless it is specifically designed by the SP and security protocols are enabled (i.e., IP security (IPSec) traffic between the evolved universal terrestrial radio access network (EUTRAN) and EPC is not secured that can allow attacker to gain access to unprotected traffic for performing malicious activities [19, 20].

Over-billing attacks (IP address hijacking or spoofing): An attacker can take control of the IP address of a legal UE while it is being returned to the IP pool and can explore the UE's data. Alternately, an over-billing attack can exist when an IP address is maliciously reassigned to another UE[20]. Preventative measures:

- Security architecture: virtual local area networks (VLANs) and virtual private networks (VPNs)
- Encryption and IKE/IPSec
- Load balancing

Security architecture: IPSec was recommended by the 3GPP to address IP based vulnerabilities. Moreover, the Next Generation Mobile Network Alliance recommends that the service providers implement VPNs in order to secure transmission in their EPC of LTE networks. This helps by isolating the signaling to the paths defined by the VLAN. As a result, unauthorized access, eavesdropping, and spoofing attacks are limited [21].

Encryption IKE/IPSec: For prevention of IP based attacks and over-billing attacks, SP can include IKE/IPSec mechanisms in their accounting, authorization and authentication processes and also in the process of securing the integrity and confidentiality [22].

Load balancing: SPs must adopt load balancing measures to protect their networks, particularly the EPC, from the signal surges. The load balancing mechanism will also help in implementing traffic volume policies, shaping and traffic prioritization. This could lead to reduced DoS attacks. Moreover, a hop-by-hop analysis within the EPC elements will ensure higher levels of security [22, 23].

2.2. Denial of Service

DoS attack is the attempt to make the networks' resources unavailable to its intended UEs. It refers to the continuous efforts of attackers to prevent a proper allocation service from functioning efficiently, temporarily, or permanently [16].

Considering SPs employing virtualization, attackers would be able to widely attack UEs since SPs' RBs would be clearly shared within the same eNB. The most common method of attack is saturating the eNB with communications requests, which makes it unable to allocate RBs, or make it respond slowly to its intended UEs so that they will no longer be able to communicate adequately. DoS attacks can silently downgrade LTE UEs by limiting their access to LTE service or limiting them from all networks' services.

During a tracking area update (TAU) procedure, the UE and its associated MME will be able to agree on the services' modes which are required to control UE mobility in the entire LTE networks, and network capabilities supported by the UE and SP. This allows the MME of the LTE network to be able offer necessary network services to the UE.

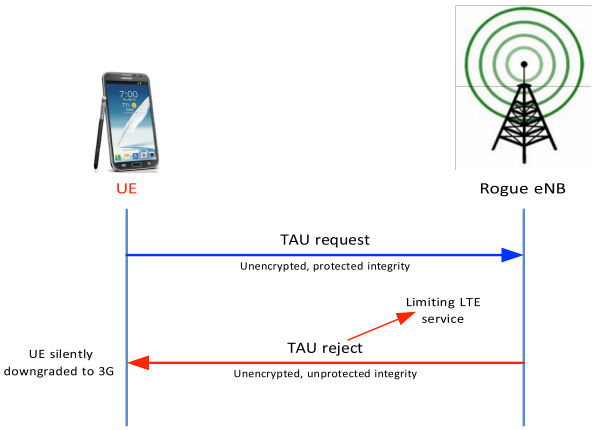
For this purpose, UE will always notify its MME about its current TA with the help of TAU request including its network modes. In this section, we will discuss two main types of persistent DoS attacks, where the attacker can exploit two important vulnerabilities, either to limit LTE, or to limit all network services to UEs.

1) **Limiting Non-LTE Services**

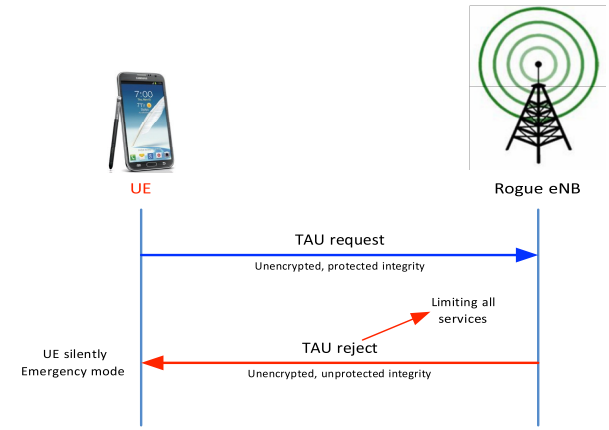
We consider that a TAU reject message that was sent from a rogue eNB is accepted by UE without any integrity protection. Assuming that, there is no implementation of mutual authentication between UEs and network for accepting reject messages, the attacker will not need any kind of security keys in order to send TAU reject messages.

As a result, UEs can be easily attacked as long as they are within the transmission distance of the rogue eNB. Similar kind of attacks are possible whenever Service reject/ Attach reject messages are used. It is shown in Figure 3-a, that the UE sends TAU request message directly to attacker's rogue eNB. Since this UE belongs to LTE network, this message can be integrity protected with the help of existing non-access stratum (NAS) security context.

Rogue eNB will be able to decode it and then respond with a TAU Reject message. As no integrity protection is required, the UE will accept the message, and as a result, the UE will not be able to use its intended LTE services[17].



(a) DoS attack: denied LTE services.



(b) DoS attack: denied all network services.

Fig. 3. DoS attack.

2. **Limiting All Network Services**

The UE initiates TAU request procedure and then the rogue eNB responds with a TAU reject message. After receiving this message, the UE sets LTE status to roaming that is not allowed and this will limit all LTE and non-LTE services until it is rebooted. Herein, UE's location is undefined to the MME and is not reachable for any network even if networks are available as shown in Figure 3-b.

3. System Model

Consider a single cell for a multiuser wireless communications in which the eNB is shared by N SPs. Where N = {1,2,...,N}. The SP is supposed to serve some active UEs where SP belongs to N and UE are represented by M_n M_n= {1,2,...,M_n} or specifically UE_{mn}. RB(av_RBs) can accessed by SPs when they are available while total number of RBs are denoted by K_n. Some frequently used notations are defined in Table I.

3.1. Transmission Block Size

LTE network looks into time and frequency domain for each RB that are constituted by looking at available bandwidth. Each sub frame has 1ms duration and consists of a contiguous set of 12 sub-carriers (180 kHz with a sub-carrier spacing of 15 KHz) that uses orthogonal frequency division multiplexing (OFDM)
[24].

The overall transport block (TB) size is a function of the spectral efficiency (ζ_s). The total TB size is given by:

$$T_{mn,k,s}(t) = \mathrm{b12}(N_{sys} - N_{OH}) \times \zeta_s(t) \times \mathrm{kc}, \quad (1)$$

Where, $N_{symbols}$ are number of symbols for each subframe, Number of overhead symbols (usually three) are represented by Table 1.

Thus, size of TB will be:

$$T_{m_n,k,s}(t) = [132 \times \zeta_s(t) \times k], \quad (2)$$

while number of RBs will be:

$$k = \frac{T_{m_n,k,s}+e}{132\,\zeta_s(t)}, \quad (3)$$

where $0 \leq \epsilon < 1$. A block error rate of 10% is allowed as signal to noise ratio (SNR) for TB delivery [24]. Figure 4 shows the spectral efficiency and TB size versus SNR.

Table 1. Frequently Used Notations

Notation	Definition
k_m	All possible RBs allocation for UE m
F_t	Finite time length of transmission time interval
k	(TTI)
K_n	RB
K_{tot}	Total number of RBs in SP n
m	Total number of RBs in all SPs
m_n	UE
M_n	UE m in SP n
M_{tot}	Total number of UEs in SP n
n	Total number of UEs in all SPs
N	SP
s	Total number of SPs
s_{m_n}	MCS
t	MCS selected for UE_{mn}
T_{m_n}	Definite TTI
Ut_n	TB of UE m in SP n
	Utility function of SP n

$N_{OverHead}$. Additional overhead can be taken by $N_{OverHead} \geq 0$ for each TB. $N_{symbols}$=14 are represented where there are 11 symbols per sub carrier in a duration of $T_s = 66.7\mu s$. There are 132 OFDM symbols per subframe [25].

3.2. Traffic in Wireless Systems

The eNB supports multiple traffic types established through multiple radio bearers per UE.This research considers three different classes of service with different packet delay and jitter requirements.

Expedited forwarding (EF) model provides resources with constant bit rate tranissmion for voice in order to handle realtime applications [13, 26]. Assured forwarding (AF) model is used for application that can manage delay a bit, like video streams applications. For this best effort delivery (BE) is used with giving file transfers a lower priority. [13].

3.3. Considered Scheduling Algorithms

eNB replies after assigning active UEs to the available RBs and reply back with the information related to RB and its power control.This research considers channel quality indicator (CQI), sounding measurements, QoS of each bearer, and TB size. In [13, 27], many schedulers are discussed. These schedulers compare data throughput, delay, fairness, and other QoS parameters. Finding the operation

perfromace for scheduling algorithm is key goal of research. For this the allocated RBk to UEm will be

$$mt_{m,k} = \max_l\{mt_{l,k}\} \quad (4)$$

where $\{K\}$ is a set of RB to be accessed by RB.

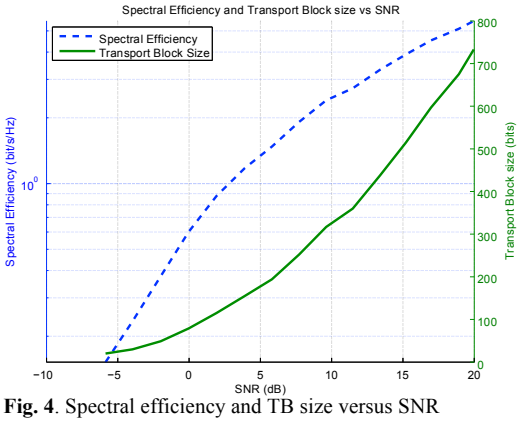


Fig. 4. Spectral efficiency and TB size versus SNR

Framework proposed here is for two SPs: SP-first cares about applying fairness between UEs while prioritizing compliance among traffic bearers. Hence, it applies strict priority (S.P.) scheduling [13]. Largest weighted delay (used for SP-Second) first look into packet tranismission with guaranteed delay but the delay is not more than packet droprate.

SP algorithm will do the scheduling based on traffic class with pirority level $i = \{1,2,3\}$ refers to EF, AF, and BE respectively. LWDF will make sure that traffic will reach before droptime thus increasing the UE performance to be flexible. While the system parameter for δ_i, the probability acceptable m^{th} for receiving the data by UE will

$$W_{im} = \alpha_{im} \times D_{HOL,im} \quad (5)$$

$$\alpha_i = \frac{-\log(\delta_i)}{T_i} \quad (6)$$

Figure 5 reperent SP and LWDF Where trafic class i will have traffic class $D_{HOL,im}$.

This goal is reached by including the specific packet arrival, processing timing, and its deadline. LWDF is used by operating systems and networks with higher bandwidth [13]. While near expiration time the priority changes to make sure message is delivered.

Only one MCS was considered for the RBs of all allocated users at transmission time interval (TTI) t. The resources are allocated according to internal policy of scheduler.

4. Problem Formulation

Multiple SP are included in a radio access network while each have different service level agreement (SLA) on the basis of which scheduling is done. There are unique nRB for each SP such that

$$K_n \cap K_u = \phi, \quad \forall n, u \in N \quad (7)$$

This research considers two form of sharing resources (a) static sharing (SS) only eNB is shared without radio resources (2) Dynamic sharing (DS) the radio resources i.e. spectrum is also shared.

4.1. Static Sharing Allocation (SSA)

Each Sp will do the scheduling itself [26]. SSA can be represented by following equation:

$$max \sum_e \sum_{j=1}^{J} \sum_{m_n=1}^{M_n} \sum_{r \in K} Ut_{m_{j,r}}(e)\psi_{m_{j,r}}(e) \quad (8)$$

Subject to

$$\sum_{j=1}^{J} \sum_{m_j=1}^{M_j} \sum_{r \in K} \psi_{m_{j,r}}(e) = 1, \quad \forall e, k \in K_j \quad (9)$$

$$\psi_{m_{j,r}}(e) \in \{0,1\}, \quad \forall m_j, r, e \quad (10)$$

Equation (8) shows the function for maximum utility for all UE where decision inputs are U_t and ψ. The allocation of RB is checked by Boolean variable $\psi_{mt,k}$.

Equations (9, 10) show the constraints about when the RB can be allocated to UE.

4.2. Dynamic Sharing Allocation (DSA)

In DSA the spectrum is also shared as well as physical RB. The allocation in DSA is shown in Equation (11) that shows the maximum objective function:

$$max \sum_{e=1} \sum_{m=1}^{M_{tot}} \sum_{r \in K} Ut_{m_{j,r}}(e)\psi_{m_r}(e), \quad (11)$$

that can be reduced as

$$\sum_{m=1}^{M_{tot}} \sum_{r \in K} \psi_{m,r}(e) = 1, \ \forall e, k \in K_{tot} \quad (12)$$

$$\psi_{m,r}(e) \in \{0,1\}, \quad \forall m, r, e \quad (13)$$

Similarly, Equations (12, 13) show the $\psi_{m,r}$ that is binary check for allocation of RB and spectrum.

5. Simulation Results

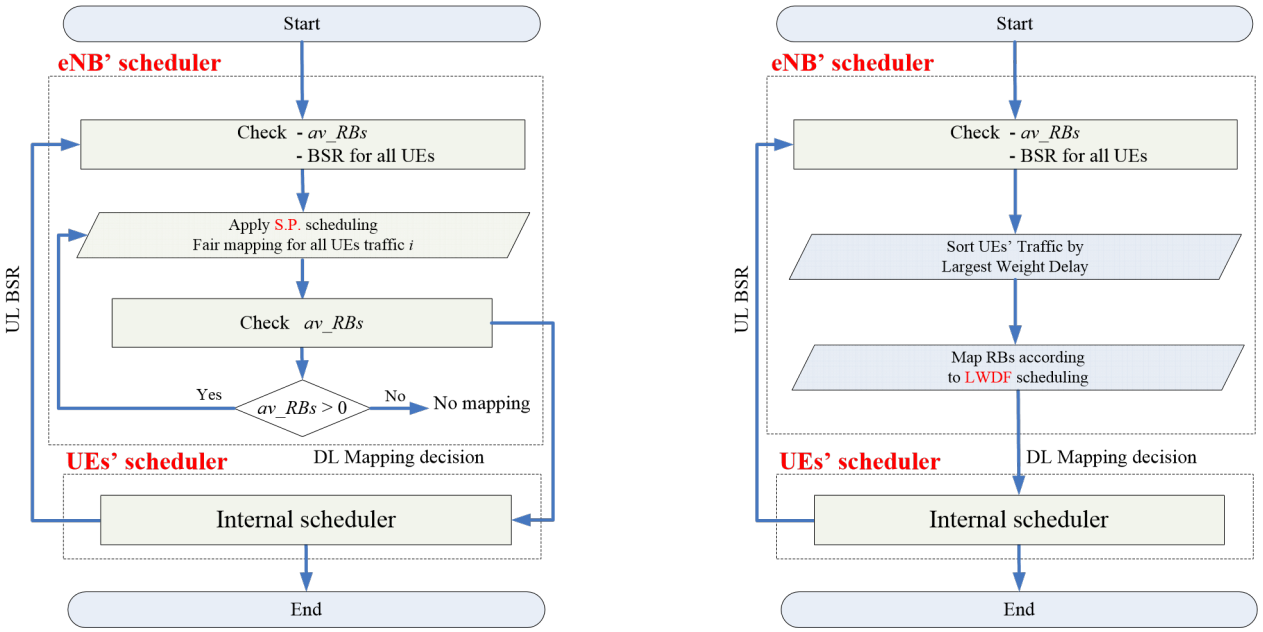
MATLAB was used to test both schemes presented with considering discrete event simulator. List are simulation parameters are described in Table II.

DS scheme as compared to SS scheme is evaluated where more number of RBs can be allocated.

Basic assumption is (a) traffic is evenly disturbed to all RB and each UE is contributing to similar amount of traffic. (b) The UE are mobile at max 3km/hr speed. (c) For each Sp one UE is in close to eNB and other is far from eNB thus in total two with average SNR SNR_l.

Figure 6 compares the throughput of the S.P. and LWDF schedulers, which shows that the LWDF scheduler improves on the throughput of the S.P. scheduler, especially with the increase in number of UEs (over 17 UEs). Average packet delay for EF and non-EF is shown in Figure 7 and it shows that non-EF have higher delay due to higher amount of traffic. EF traffic may not be able to achieve QoS due to

limited support of UE. This could be handled by SP-1, as it can go over 50 UEs because it is the S.P. for the EF traffic application.



(a) Strict priority scheduling algorithm. (b) Largest weight delay first scheduling algorithm.

Fig. 5. The services' providers scheduling algorithms.

However, UEs are treated differently within the same channel quality [28]. This is because of the different scheduling algorithms applied by the SPs. To reiterate, UE-1 and UE-3 have the same low channel quality (SNR_l), and UE-2 and UE-4 have the same high channel quality (SNR_h). Average packet delay before sharing resources for SP-two scheme is shown in Figure 8.

Figure 9 shows the DS scheme, where the SLA has a different resource sharing weight for each SP. Such a scenario might happen when SPs with different budgets share the same eNB [13]. For resource sharing (w) for SP-1 20% weight is assigned for sharing resources. RBs may be borrowed (shared if they are not used by SP-1) by SP-2.

Table 2. Simulation Parameters and Values.

Parameter	Value
Spectrum allocation	20 MHz
Carrier frequency	2 GHz
Number of subcarriers per RB	12 subcarriers
Neighboring subcarrier spacing	15 KHz
RB bandwidth	180 KHz
Slot duration	0.5 ms
Cell radius	1 Km
MCS	QPSK, 16QAM, 64QAM
UEs in SP-1	2 UEs (UEs-1, and 2)
UEs in SP-2	2 UEs (UEs-3, and 4)
RBs available in SP-1	10 RBs
RBs available in SP-2	10 RBs
SP-1 scheduler	S.P.
SP-2 scheduler	LWDF
Channel fading	Rayleigh
Iteration #	1e4
Channel Estimation	Perfect
SNR_h (UEs-2, and 4)	15 dB
SNR_l (UEs-1, and 3)	10 dB
Coherence time	1 ms
Cells interference	Avoidance

Similarly, the resource sharing weight for SP-two 40% of the resources of the SP-2 RBs may be shared with SP-1. As a result, SP-1 can use 14 RBs and SP-2 can use 12 RBs for their users (if they are free and not allocated by the UEs of the SPs in this TTI). Experimental results revea that delay is traffic is significantly reduced compared to traditional schemes.

Throughput comparison of different scheduling schemes

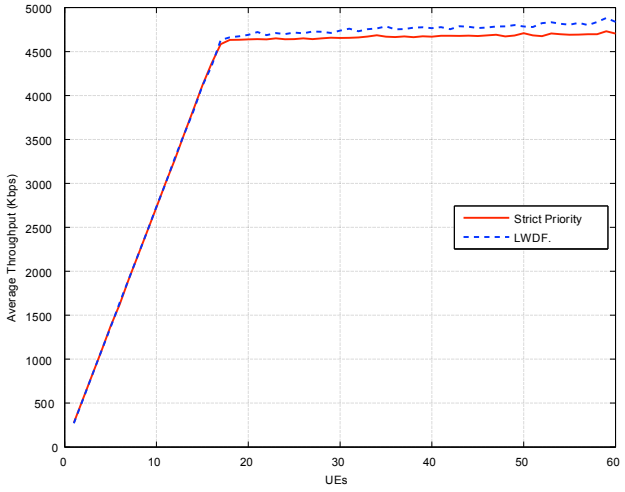


Fig. 6. Average throughput of the S.P. and LWDF schedulers.

Figures 10 and 11 present the effect of weighted sharing on the AF and the average BE packet delay. These results confirm that increasing factor w enhances QoS. That can save up to 47 % for SP-1 and 64 % for SP-2 in the AF traffic average packet delay. And, it can also save up to 65 % for SP-1 and 80 % for SP-2 in the BE traffic average packet delay.

To better visualize the effect of the security issues on the allocation algorithm, we assume that the virtualized allocation between SP-1 and SP-2 (with their considered weights) is attacked by DoS attacker, who aims to deny the performance of non-EF traffic for all UEs. Figure 12 shows

the experimental results before attack for both kind of traffics. It is clear that DS scheduling has less average delay than the SS for all types of traffic services. It also shows the performance of SP-1 over SP2 in terms of the delay parameter.

The EF traffic for SP-1 and SP-2 performing DS are overlapped with an average packet delay of 1 ms. While, they differentiating from the SS case with improvement in the average packet delay.

While after attack (DoS attack) the average packet delay is shown in Figure 13. It shows the effect on the non-EF traffic increasing in queue size, where UEs update their queues and send their BSR to the eNB, requesting RBs allocation without being able to process their data. However, with the considered DoS attack, the available RBs are all allowed to be allocated to the EF traffic services, leading to enhance their average packet delay.

6. Conclusion

This research work discusses a trade-off between the security and virtualized schemes for downlink LTE systems that advantageously complement the infrastructure mode. In this study, RB sharing techniques for SPs on a single eNB were investigated. QoS requirements for different classes of services along with channel fading parameters were considered to do performance analysis. This paper also provided an overview of the key security risks that can affect an LTE structure that deploys virtualization as well as their preventative measures.

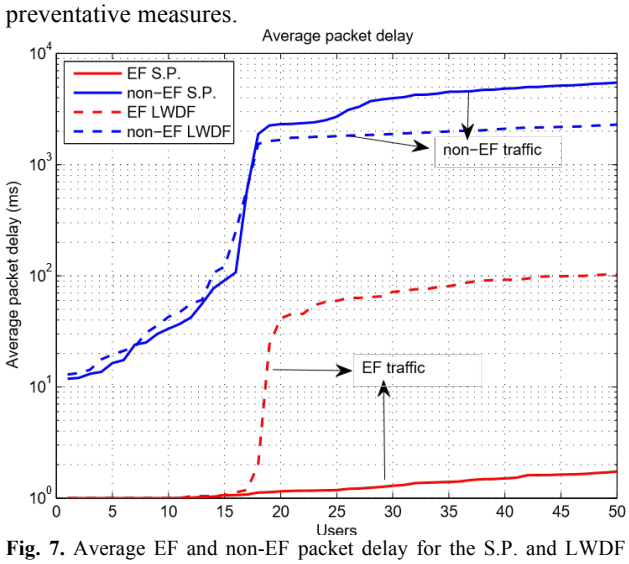


Fig. 7. Average EF and non-EF packet delay for the S.P. and LWDF schedulers versus the number of UEs. Bearers delay achieved with non−sharing approach

Evaluation the average packet delay and jitter for both the SS and DS schemes is provided that aims to limit the growing gap between the actual capacity in the backbone networks compared to the critical access infrastructures that connect the end-user networks. Overall, the simulation results prove that the DS framework provides notable improvements in average packet delay because of the larger pool of RBs available for the UEs. This improvement will help SPs to customize their efforts in order to schedule and control the sharing of their entire resource pool.

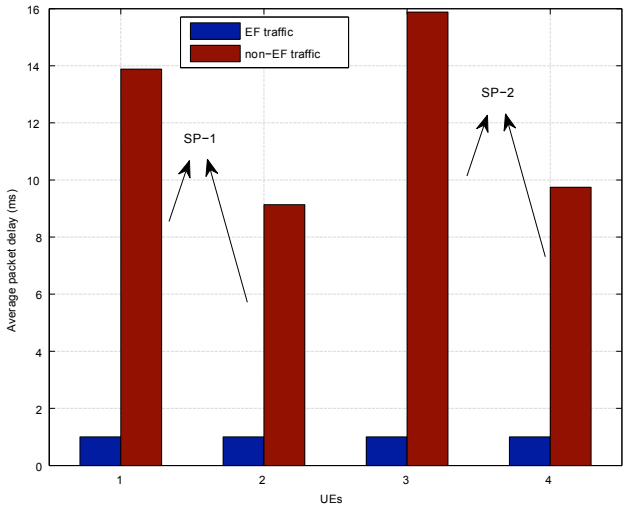


Fig. 8. Average packet delay in SP-1 and SP-2 before sharing resources.

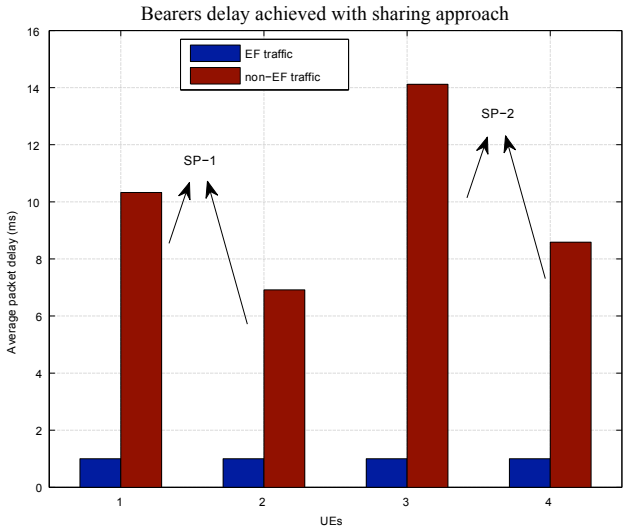


Fig. 9. Average packet delay in SP-1 and SP-2 after sharing resources.

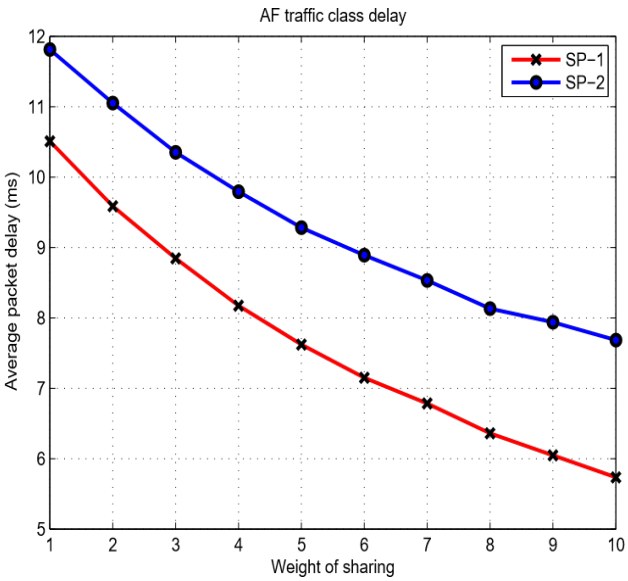


Fig. 10. Average AF packet delay with respect to various resource sharing weights.

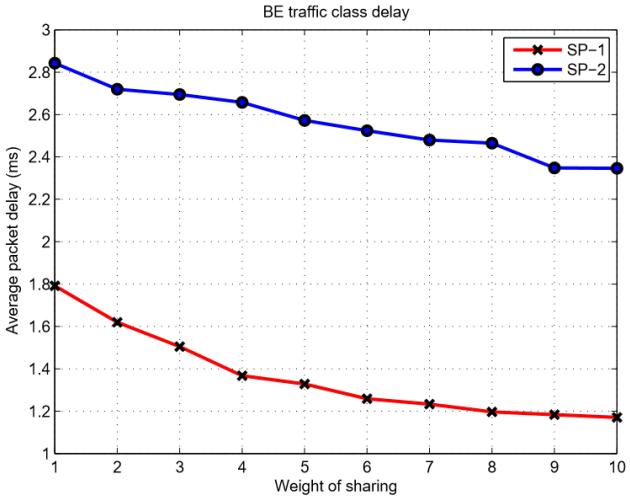


Fig. 11. Average BE packet delay with respect to various resource sharing weights.

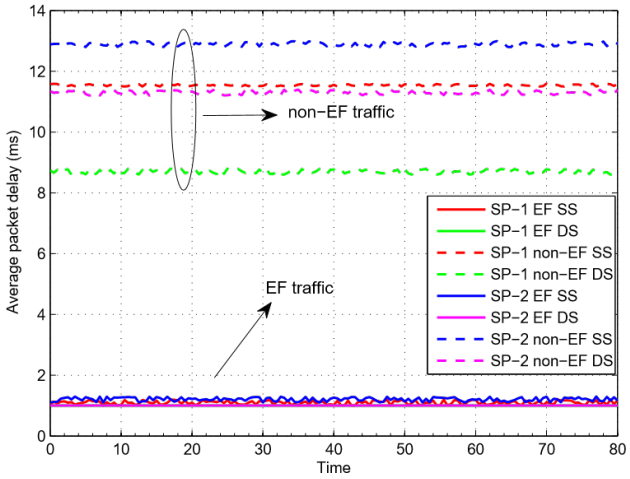


Fig. 12. SPs' average packet delay without DoS attack. SPs average packet delay with DoS attack

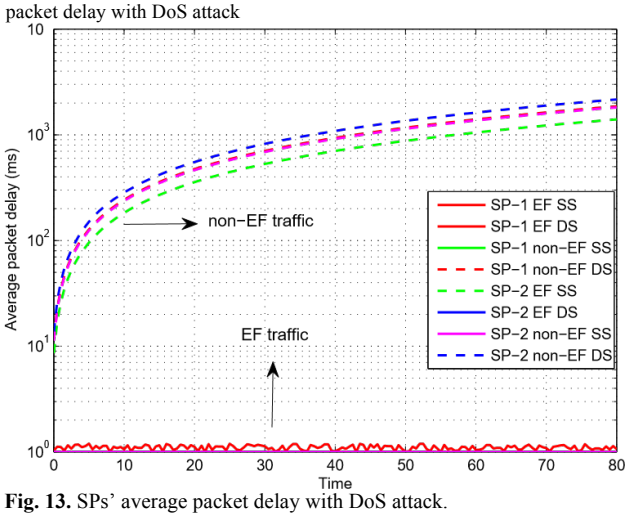


Fig. 13. SPs' average packet delay with DoS attack.

Acknowledgments

This research is sponsored by King Abdulaziz City for Science and Technology (KACST).

This is an Open Access article distributed under the terms of the Creative Commons Attribution Licence

References

1. M. Peng, Y. Sun, X. Li, Z. Mao, and C. Wang, "Recent advances in cloud radio access networks: System architectures, key techniques, and open issues," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2282–2308, 2016.
2. D. Bhamare, M. Samaka, A. Erbad, R. Jain, L. Gupta, and H. A. Chan, "Optimal virtual network function placement in multi-cloud service function chaining architecture," *Computer Communications*, vol. 102, pp. 1–16, 2017.
3. C. Liang and F. R. Yu, "Wireless network virtualization: A survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 358–380, 2015.
4. M. Wang and Z. Yan, "A survey on security in d2d communications," *Mobile Networks and Applications*, vol. 22, no. 2, pp. 195–208, 2017.
5. H. Sun, Z. Zhang, R. Q. Hu, and Y. Qian, "Challenges and enabling technologies in 5g wearable communications," *arXiv preprint arXiv:1708.05410*, 2017.
6. Y.-P. E. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi, "A primer on 3gpp narrowband internet of things," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 117–123, 2017.
7. N. Saxena, A. Roy, B. J. Sahu, and H. Kim, "Efficient iot gateway over 5g wireless: A new design with prototype and implementation results," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 97–105, 2017.
8. M. Alam, D. Yang, J. Rodriguez, and R. Abd-alhameed, "Secure device-to-device communication in lte-a," *IEEE Communications Magazine*, vol. 52, no. 4, pp. 66–73, 2014.
9. S. Shin, H. Wang, and G. Gu, "A first step toward network security virtualization: from concept to prototype," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2236–2249, 2015.
10. N. Prasad, H. Zhang, H. Zhu, and S. Rangarajan, "Multiuser scheduling in the 3gpp lte cellular uplink," *IEEE Transactions on Mobile Computing*, vol. 13, no. 1, pp. 130–145, 2014.
11. E. J. Kitindi, S. Fu, Y. Jia, A. Kabir, and Y. Wang, "Wireless network virtualization with sdn and c-ran for 5g networks: Requirements, opportunities, and challenges," *IEEE Access*, 2017.
12. S. Jasper and J. Wirtz, "Cyber security," in *The Palgrave Handbook of Security, Risk and Intelligence*. Springer, 2017, pp. 157–176.
13. M. Hussein, S. Primak, and A. Shami, "On sharing resources performance analysis in 3gpp-lte systems framework," in *International Wireless Communications and Mobile Computing Conference (IWCMC), 2015*. IEEE, 2015, pp. 302–307.
14. A. A. Atayero, M. K. Luka, M. K. Orya, and J. O. Iruemi, "3gpp long term evolution: Architecture, protocols and interfaces," *International Journal of Information and Communication Technology Research*, vol. 1, no. 7, pp. 306–310, 2011.
15. C. Basile, A. Lioy, C. Pitscheider, F. Valenza, and M. Vallini, "A novel approach for integrating security policy enforcement with dynamic network virtualization," in *1st IEEE Conference on Network Softwarization (NetSoft), 2015*. IEEE, 2015, pp. 1–5.
16. L. R. Battula, "Network security function virtualization (nsfv) towards cloud computing with nfv over openflow infrastructure:

Challenges and novel approaches," in *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*. IEEE, 2014, pp. 1622–1628.

17. A. Khan, Y. Javed, J. Abdullah, J. Nazim, and N. Khan, "Security issues in 5g device to device communication," *IJCSNS*, vol. 17, no. 5, p. 366, 2017.
18. R. Anand, S. Sarswathi, and R. Regan, "Security issues in virtualization environment," in *Radar, Communication and Computing (ICRCC), 2012 International Conference on*. IEEE, 2012, pp. 254–256.
19. P. Chau and Y. Wang, "Security-awareness in network virtualization: A classified overview," in *Mobile Ad Hoc and Sensor Systems (MASS), 2014 IEEE 11th International Conference on*. IEEE, 2014, pp. 545–550.
20. W. K. Leong, A. Kulkarni, Y. Xu, and B. Leong, "Unveiling the hidden dangers of public ip addresses in 4g/lte cellular data networks," in *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications*. ACM, 2014, p. 16.
21. S. Shin, H. Wang, and G. Gu, "A first step toward network security virtualization: from concept to prototype," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2236–2249, 2015.
22. J. Kerdsri and K. Wipusitwarkun, "Data-wise routing in virtualization environment (drive) with multiple level of security for tactical network," in *IEEE/SICE International Symposium on System Integration (SII), 2012*. IEEE, 2012, pp. 933–938.
23. M. Li, L. Zhao, X. Li, X. Li, Y. Zaki, A. Timm-Giel, and C. Gorg, "Investigation of network virtualization and load balancing techniques in lte networks," in *IEEE 75th Vehicular Technology Conference (VTC Spring), 2012*. IEEE, 2012, pp. 1–5.
24. M. Hussein, A. Moubayed, S. Primak, and A. Shami, "On efficient power allocation modeling in virtualized uplink 3gpp-lte systems," in *Wireless and Mobile Computing,*

Networking and Communications (WiMob), 2015 IEEE 11th International Conference on. IEEE, 2015, pp. 817– 824.

25. D. J. Dechene and A. Shami, "Energy-aware resource allocation strategies for lte uplink with synchronous harq constraints," *IEEE Transactions on Mobile Computing*, vol. 13, no. 2, pp. 422–433, 2014.
26. M. Hussein, A. Moubayed, S. Primak, and A. Shami, "Virtualized allocation performance analysis in 5g twotier cellular networks," in *IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2016*. IEEE, 2016, pp. 1–4.
27. F. Capozzi, G. Piro, L. A. Grieco, G. Boggia, and P. Camarda, "Downlink packet scheduling in lte cellular networks: Key design issues and a survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 678–700, 2013.
28. P. K. Korrai and D. Sen, "Performance analysis of ofdm mmwave communications with compressive sensing based channel estimation and impulse noise suppression," pp. 1– 6, 2016.