Future 5G Mobile Broadband Networks Using Cloud-based Services with Advanced Security and QoS Framework

Mitko Bogdanoski[1], Tomislav Shuminoski[2], Metodi Hadji-Janev[1], Aleksandar Risteski[2], Toni Janevski[2]

[1]Military Academy "General Mihailo Apostolski" University of Goce Delcev, an associated member, Str. Vasko Karangeleski BB 1000, Skopje, Macedonia
[2]Ss. Cyril and Methodius University, Faculty of Electrical Engineering and Information Technologies, Rugjer Boshkovik 18, PO Box 574, 1000 Skopje, Macedonia
E-mails: mitko.bogdanoski@ugd.edu.mk, tomish@feit.ukim.edu.mk, metodi.hadzi-janev@ugd.edu.mk, acerist@feit.ukim.edu.mk, tonij@feit.ukim.edu.mk

Abstract: The work suggests a potential solution to contemporary Corporate and National security concerns, with regards to the use in the future of 5G technologies. In today's digital age, individuals, groups and some states, (ab)use the easy access to modern technologies to further their economic and political objectives. In these endeavors, among others, these actors utilize jamming attacks (i.e. electronic warfare tactics exclusively used by the military in the past), in order to produce the well-known effect of DoS (Denial of Service). Up to now there is no communication technology that is immune to the jamming attacks, so there is no expectation that the new 5G concept, that is still under development will be fully resistant to well-known traditional jamming and other types of attacks. The proposed Security and Quality of Service (QoS) framework provides high levels of security features and safety, through high-performance mobile broadband networks, using Mobile Cloud computing. It guarantees QoS provisioning for different broadband services, with present jamming, as well as, other types of distributed DoS (DDoS) attacks. Moreover, the trend of integrating various criminal activities in the cyberspace is also presented. The performance of the proposed security and QoS framework is evaluated through simulations and analysis with multimedia traffic, in a heterogeneous mobile broadband Cloud environment with the coexistence of multiple radio technologies.

Keywords: 5G; Cloud; Cyber; Jamming; DoS; Quality of Service (QoS); Security

1 Introduction

The advancement of modern mobile and wireless technology and its usage in attending political objectives have changed threat perceptions, definitions of weapon systems and the way of achieving strategic-political objectives. Although the use of modern-day technologies and cyberspace provide many benefits there are numerous examples where individuals, groups and even states have abused modern technologies and cyberspace in achieving strategic ends. These tendencies have urged countrywide and corporate security risk management teams to change the approach to the threat vectors. Consequently, new threat vectors in the digital age are blurring the line between peace and war. This is understandable giving that modern technologies have changed the idea of weaponry arsenal at potential adversaries' disposal. The cyber-attack(s) understood as syntactic (straight forward-viruses, worms, Trojans, etc.), semantic (the modification and dissemination of correct and incorrect information) or combination, can be serious weapon system. This weapon system can be used for achieving different end-states. The threat level that these weapons can cause in time, space and effects are significant.

One example that has a widespread implementation in modern battlespace activities and is as old as the emergence of radio equipment, it is called the "jamming" process. This process, because of its nature and method of operation belongs to the well-known group of attacks called DoS (Denial of Service). Up to now there is no communication technology that is immune to the jamming attack, so there is no expectation that the novel 5G concept that is still under development will be fully resistant to the well-known traditional jamming attacks. The importance of defining the security measures for the new 5G device-centric based technology [1-8] that is at the front door is obvious. Considering mentioned, this technology is expected to take a significant part of the Next Generation Mobile Broadband network, not bypassing the military networks [9, 10]. Taking suitable measure against different disruption in the proper functionality of the 5G technology, including the appropriate answer against the jamming attack, need to be one of the key areas during the development phase.

Indubitably, the future 5G networks would require smarter devices capable of providing a broad range of multimedia services to cell customers, with the enormous spectrum for advanced capabilities. The 5G security of wireless cellular systems is expected to be divided in the security issues for the main three services:

1. Enhanced Mobile BroadBand (eMBB)
2. Ultra-Reliable Low-Latency Communications (URLLC)
3. Machine-Type Communications (mMTC) [11-14]

The concept of our framework, presented herein, is a 5G based terminal that has access to various different radio access technologies (RATs), at the same time and

to be able to combine different secured flows from different technologies using advance security and QoS algorithms, vertical multi-homing and multi-streaming [15] [16].

The paper is organized as follows. Section 2 discusses some background researches on converging jamming and hacking in the age of cyber warfare in mobile and wireless networks and provides an overview of different types of jamming attacks. Section 3 describes the System Model together with the proposed security and QoS algorithm and a proposed method to mitigate the jamming effects. In Section 4 the simulation results and analysis are discussed. Finally, Section 5 gives some conclusions of our work.

2 Related Works

Contemporary dynamics in military affairs confirm that cyberwarfare has expanded beyond the digital realm. As the wireless networks become a norm so does the ability to attack a target simultaneously in multiple ways from multiple domains. Among others, national and corporate security risk assessment teams produce guidance that urges leadership to merge cyber warfare and traditional electronic warfare type of activities. Although jamming technologies was once the exclusive province of the military, today these technologies have become so commonplace that can be purchased online.

Parallel with the above, along with the improved performances and QoS, the brand new 5G concept should undoubtedly provide the capability to ensure security, trust, identity, reliability, and privacy, that are highly vital [17-20]. The [21] presents that any eventual security solution in the 5G should take into considerations the needs for low latency, low power, and high reliability. Moreover, there will be a very wide range of 5G use cases with different requirements, that will need to be secured and overviewed. Significant importance in nowadays and future telecommunication networks' security is to focus on mobile broadband networks and to prove the vulnerabilities in the implementation and configuration of those networks. Additional exposure of future mobile and wireless networks to attacks must be expected from the trend [22-25] away from imposing advanced RAT functions using proprietary algorithms. One challenging fact is that the 5G networks, due to the new networks of Internet of Things (IoTs) [26], Mobile Cloud Computing (MCC) [27], Software-defined networking (SDN) [28,29] and Network Function Virtualization (NFV) [30] are open doors to novel security threats [19]. Therefore, the security architectures of the 3G and 4G will not fulfill the security requirements of the 5G networks, and the securely using above-mentioned technologies and providing user privacy in future 5G networks are bringing new concerns, new demanding situations and new challenges. Moreover, the MCC in 5G has emerged as a key and most significant paradigm,

promising to augment the capability of mobile terminals through provisioning of computational resources on demand, and enabling cell users to offload their processing and storage requirements to the Cloud servers [31].

In that way, a converged access-agnostic core (where identity, mobility, security, etc. are decoupled from the access technology), which integrates fixed and mobile core, is envisioned as a direction of IMT-2020 [32, 33]. Therefore, the IMT-2020 network architecture proposed by ITU (International Telecommunication Union), should be studied to support a true fixed and mobile convergence ensuring a seamless user experience within the fixed and mobile domains. The most significant example of 4.5G: LTE-Advanced Pro provides a smooth transition to 5G New Radio (NR) to meet IMT-2020 requirements given from ITU [34].

Different from the other related works, this paper provides Security and Quality of Service (QoS) framework that can result in a high level of security features and safety through high-performance mobile broadband networks. The proposed framework guarantees QoS provisioning for different multimedia services (including video, audio, and data), with present jamming and distributed denial-of-service (DDoS) attacks (i.e. the jamming attacks).

However, before we provide an explanation for our proposal it would be useful to take a brief summary of the different types of jamming attacks.

2.1 Types of Jamming Attacks

There are several distinct classifications of the jamming attacks [35-37]. In the classification we adopt [38-40], seven jamming models are defined. The most common model is the constant jamming. This model describes the continuous signal or noise transmission to interfere with other ongoing transmissions. Deceptive jamming is very similar to the constant jamming, and the similarity is that both constantly transmit bits. Unlike the constant jamming, the transmitted bits in deceptive jamming are not random. The deceptive jamming continually injects regular packets on the channel without any gaps between the transmissions. Busy jamming is the type of jamming where a very short pulse of noise is created for every interval that is less than DIFS (Distributed Inter-Frame Space), so the nodes are fooled into thinking that the medium is busy. In order to save energy and reduce the probability of detection, other jamming techniques as bursty or random jamming are used, where jamming signals transmission is less frequently. On the other hand, reactive and corruption jamming are the most "intelligent" jamming techniques which only transmit whenever an ongoing transmission or a certain message is sensed. None of the recent known mechanisms are capable enough to handle the jamming attack on wireless networks [41]. An ideal jamming attack should have high energy efficiency (i.e., consume low power), low probability of detection, achieve high levels of DoS (i.e., disrupt communications to the desired extent) and be resistant to PHY layer anti-jamming techniques [42].

3 System Model and ASECQUA Algorithm

The system model of our proposed framework for secure 5G node is shown in Figure 1. The 5G node is using network aggregation and is using all available RAT interfaces. The entire framework is placed in both nodes: the mobile terminal node and fixed node (secure and QoS server) in the core network, with several (n) interfaces (each for distinctive RATs) as shown in Fig. 1. The developed determined framework is based on advanced Security and QoS provisioning algorithm, set within a module on network layer with advanced user-centric aggregation algorithm using vertical multi-homing and multi-streaming capabilities [15] [16] and [43-45]. According to network congestion and security conditions, it selects the most suitable, most reliable and most secure RAT/RATs per used service. We refer to it as Advanced Security QoS-based User-centric Aggregation (ASECQUA) algorithm, which is defined independently from any existing or future technology below network layer. The functionalities with more information and details for the QoS part of the AQUA module are elaborated in [43] and [44], and for the security part in the [45].

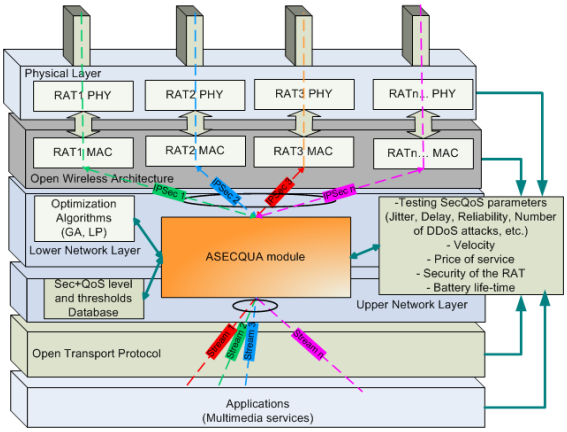

Figure 1

System model for the Secure 5G node with ASECQUA algorithm

The fundamental novelty and distinction from our previous works [43-45] is the development of new advanced Security and QoS Module with improved testing parameter module, IPSec key entity, and Sec+QoS level and thresholds Database, using vertical multi-homing and multi-streaming security features. It uses Multi-RAT interfaces and IPSec encapsulation, where IPSec key entity helps with holding parameters (such as keys) that are used to encrypt and authenticate a particular flow, in the process of forming the IPSec security associations. The information for the network congestion, security, and overall conditions is stored in ASECQUA Cloud server (the Sec+QoS level and thresholds Database) that is a fixed node placed in the core part of the network, due to higher processing and

memory requirements. This information can be: number of users connected per RAT, number of jamming (as one particular type of DDoS attack) attacks per RAT, jamming attack information, the volume of used capacity per RAT, RAT reliability, RAT availability, level of the security threats and etc. Also, the mobile node can have a smaller similar Database, only with collected and necessary information. The module considers the predefined thresholds for the observed parameters, in order to choose the most appropriate optimization algorithm (i.e. the GA (Genetic Algorithm) or LP (Linear Programming) algorithm, stored in the Optimization Algorithms database). To emphasize, ASECQUA is a novel crucial component in our system model, complementary to our previous work in this field ([43-45]), but improved with new security features. That gives profound advantages and better security traffic control for real-time and non-real-time broadband services. It uses different IPSec encapsulation and keys for each different traffic streams (IPSec flow 1, IPSec flow 2, etc.) in Tunnel or Transport mode. Optionally, the mobile node can use one overall IPSec encapsulation (in transport mode) in the Upper IP Layer for better security in an uplink. The ASECQUA proxy server, on the other side (in the core network), will do the IPSec de-capsulation for all streams and will forward the traffic streams in the core part of the network, Internet or other legacy cellular networks.

3.1 ASECQUA Algorithm

Looking the ASECQUA algorithm, one might also be aware the data measurements for different selection criteria, which include user requirements, Security and QoS requirements, operator requirements, as well as radio link conditions, DDoS attacks, jamming attacks (see the following subsection) and other security threats in different RATs presented with n inputs as n sets of parallel criteria functions (CFs), one set per each RAT (from RAT 1 to RAT *n*). One RAT CF is shaping and filtering the outputs from the previous components into adequate interior threshold functions. The ASECQUA module has capability to select one Optimization Algorithm (OA), which as inputs uses: the outputs of the *n* sets of parallel CFs, five values from each RATs (5*n in total) and the output of the threshold CF for battery support (one value) which shapes and filtrates the outputs from the user's mobile battery lifetime. In the process of choosing the algorithm (GA, LP, or other OA) for optimization of the weighted factors, the ASECQUA module is doing the optimal and appropriate choice of algorithm, depending on the different input criteria and conditions for each RAT, for given service, by coordination of the other entities and mentioned Database.

Finally, the ASECQUA module, besides other mentioned functions, is centered for the selection of RATs, so the outcome choice should select the high-quality and most suitable (stable and secure) RAT or RATs with the highest value for a RAT ranking function (1). The *i*-th RAT ranking function is calculated as follows:

$$RF_{RAT\,(i)} = \frac{SECt_i \cdot W_{SEC} + QoSt_i \cdot W_{QoS}}{W_{SEC} + W_{QoS} + W_C + W_V + W_{SS} + W_B} + \frac{Ct_i W_C + Vt_i \cdot W_V + SSt_i \cdot W_{SS} + Bt_i \cdot W_B}{W_{SEC} + W_{QoS} + W_C + W_V + W_{SS} + W_B} \quad (1)$$

for $1 \le i \le n$ and $W_{SEC} + W_{QoS} + W_C + W_V + W_{SS} + W_B = 1$ (2)

where $W_{SEC}, W_{QoS}, W_C, W_V, W_{SS}, W_B$ are assigned weight factors for the CFs of: Security attack parameter, QoS parameter, service price, velocity of the MT, signal strength, and ME battery support, respectively. Those values of weight factors are assigned using a particular method of optimization. On the other hand, after passing the interior threshold functions for *i*-th RAT CF, the outputs (shaped values as real numbers within the limits [0, 1]): $SECt_i$ are regarding for the Security parameters, QoS parameters are QoSti, from service price are Ct_i, from velocity support are Vt_i, and from detected signals strength are SSt_i. The shaped output value of the threshold CF for battery support is Bt_i. So, the final step is selection of the optimal and the most secure RAT(s) for a given service or stream (if we have done multi-streaming before):

$$\max_{service\_m} \left\{ Optimal\left(RF_{RAT\,(i)}\right) \right\} \quad (3)$$

subject to: $W_{SEC} \le 1,\ W_{QoS} \le 1,\ W_C \le 1,\ W_V \le 1,\ W_{SS} \le 1,\ W_B \le 1$ (4)

and (2), for $1 \le i \le n;\ 1 \le m \le 3$ (5)

Above we have defined the optimization problem, where service_m is the given service (i.e. *m*=1 for audio, *m*=2 for video and *m*=3 for data), and Optimal (RF_{RAT_i}) is the optimal function value for the *i*-th RAT RF, calculated by OA (which reaches the global optimum).

3.2 Adaptive Transmission Power and Receiver Sensitivity Adjustment Algorithm with ASECQUA

Despite many proposed countermeasures against low power jamming attacks, the best results are achieved by the combination of increased transmission power on the transmitter side, decreased receiver sensitivity (reception power threshold) and the used spread spectrum technique (iDSSS). DSSS in many scenarios is set as a default spread spectrum technique on wireless nodes and WiFi Access Points, whereby transmission power and receiver sensitivity were manually set to the given level. In our ASECQUA module, we are considering the possibility of adaptive transmission power and receiver sensitivity adjustment. In order to achieve this, we propose an algorithm working within the ASECQUA module, using the amendment 5, part 11, of the 802.11h-2003 standard [46], which considers transmitting power management, when there is a jamming attack in some particular RAT. Considering the fact that, in wireless and mobile communications, the Medium Access Control (MAC) layer is responsible for

Transmit Power Control (TPC), we are proposing this adaptive transmission power and receiver sensitivity adjustment mechanism to be implemented at the IP layer, but to have tight cross-layer connections with the Layer Two. The examined scenario in our simulation works in infrastructure mode so that most of the computation will be done by RAT AP (or Base Station if this is not WLAN RAT), which does not mean that the wireless and mobile client terminals are not able to implement this standard. All work is supported by three elements which are used for TPC solution. These three elements are TPC request element, TPC report element and Power constraint element [46]. As can be seen in [46], there are 4 octets in the TPC Report element. The information about transmission power (used to send TPC Report element back to the node, or in our case AP) and actual link margin (received transmission power from the client stations measured at the side of the AP minus sensitivity for the time when related TPC Request element was received) is contained in the last two octets. This information follows as a response to a TPC Request element. Received TPC reports are stored in AP's database, and these reports are used for the purpose of power control. Fig. 2 shows the process of measurement of the TPC for the AP. Based on the information from the TPC Report elements the AP calculates the minimum transmit power it needs to set for downlink (DL) communication with each of the wireless client stations (STAs). The AP also calculates the transmit power for each of the client stations which they should set for uplink (UL) communication with the AP. The management frame containing information about the minimum and maximum transmit power is than sent to the client stations [46].

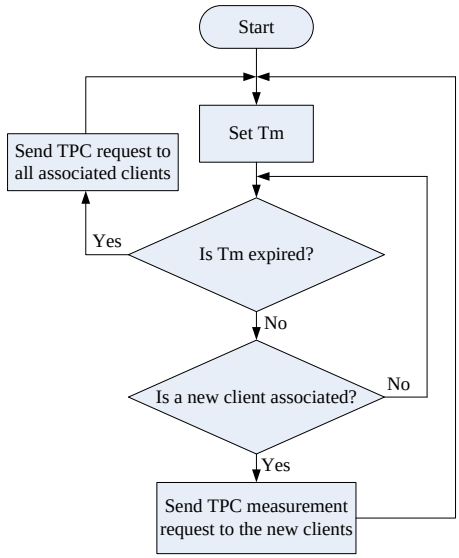

Figure 2
TPC measurement process in ASECQUA algorithm

Considering the client *n*, in order to guarantee QoS, desired received power P_{rn} is equal to:

$$P_{rn} = S_{inn} + D \tag{6}$$

where S_{inn} is the receiver's sensitivity and D is the margin to be above the receiver's sensitivity. If we replace all losses, including Free space path loss (FSPL), shadowing effects and jamming with L_n then the transmit power can be calculated as:

$$P_{RSSIn} = P_{tn} = L_n + S_{inn} + D = I_n + D \tag{7}$$

The link margin $M_n(i)$ in the TPC Report for the i-th measurement is:

$$M_n(i) = P_{rn}(i) - S_{inn} \tag{8}$$

The transmit power by the AP used to transmit data frames to client *n* is equal to P_{RSSI} or desired P_{tn}.

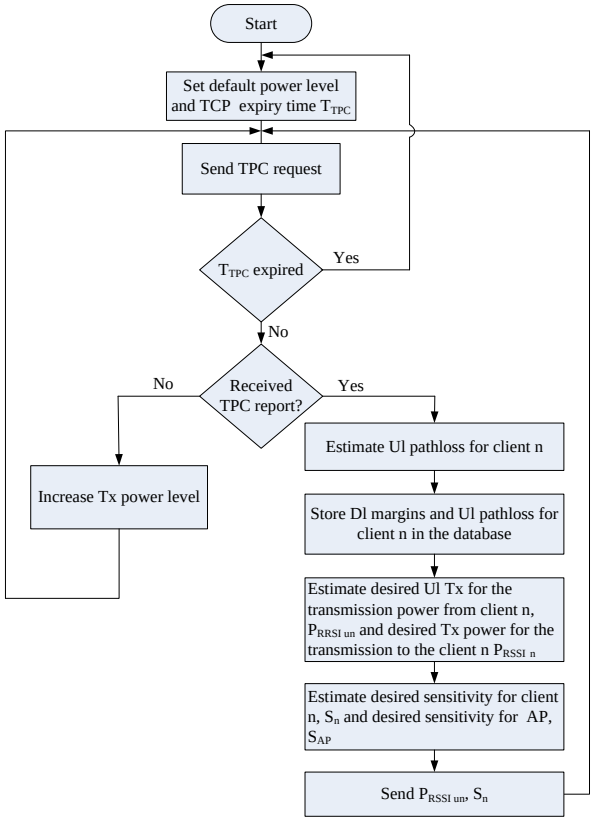

Figure 3
TPC decision based on TPC report elements from the adequate terminals in ASECQUA

The power is controlled per each client station, so for each station different transmitter power is used. Fig. 3 shows algorithm decision on AP side based on measurement reports from wireless client stations. It should be mentioned that many mobile and wireless cards do not support a change of the transmit power on the AP side, so the AP sets its transmit power based on the mobile and wireless client terminal that facing worst link conditions. In this way, the AP transmits sufficient power so the STA with worst conditions successfully receives wireless packets. If the AP is associated with many STAs, the AP's transmit power is:

$$P_t = \max_n(P_{tn}) = \max_n(P_{RSSIn}) \tag{9}$$

When the AP initializes, it transmits at default power level, that is: $P_t(0) = \max P$.

As it is shown in Fig. 3, the AP estimates path loss for client n (which will include FSPL, shadowing effects, and jamming effects), stores DL margins and UL path loss for client station, estimates its own transmission power and sensitivity, as well as STA transmission power and sensitivity. The AP also sends the estimated STA transmission power and sensitivity to the appropriate STA. If the link experiences some problems, in our case if a jamming attack occurs, the AP will not receive TPC Report, and it will iteratively increase its transmit power (each iteration will increase the power for 0.005 W). On the wireless and mobile client side, the situation is same. TPC Request/Report elements can be also implemented on STA side [46], so the STA can also iteratively increasing the power level until TCP Report from the AP is received. As it is shown in equations (6) and (7), the receiver sensitivity is also connected with transmission power, so the AP can estimate and send the best transmission power-receiver sensitivity ratio, which means that if transmission power on one site is increased, the receiver sensitivity on the opposite side can be decreased, so any noise which occurs in communication link, including the jamming signal produced by low power jammers, can be squelched.

4 Simulation Results and Analysis

The obtained simulation results for average aggregated system throughput, as well as average multimedia secure access probability values for different 5G and heterogeneous mobile and wireless broadband network conditions (with different security threats per different RATs), are presented furthermore. The jamming and DDoS attacks and the effects of these attacks are simulated in OPNET Modeler environment [40] [47-52]. The performance of the proposed ASECQUA framework is evaluated through simulations done in both MATLAB and OPNET. For solving the optimization problem (3) we are using MATLAB functions: GA when using genetic algorithm and LP when using linear programming, for finding

the optimal (maximal) RAT ranking function (1) for a given service. Moreover, the adaptive transmission power and receiver sensitivity adjustment algorithm proposed in subsection 3.2 is written in MATLAB scripts. After that, the calculations and results from MATLAB scripts and functions, using the technology of the MATLAB engine interface are integrated into OPNET, where the system model is placed.

The average aggregated system throughput is the average sum of all throughputs per mobile node, and the multimedia secure access probability ratio is calculated as the ratio of all successful and secure multimedia service access attempts from the users and the total number of all multimedia service access attempts (including not secure multimedia service access attempts due to the jamming attacks, DDoS attacks or other cyber and security threats). Our simulation scenario is a multi-cell scenario, plotted in the dense urban area, with random initial locations of MTs uniformly distributed within the entire observed area. The scenario consists of three kinds of RATs. All base stations are positioned in various locations within the simulation area, and their positions (per cell), together with their network coverage areas and capacities are given in Tab. 1. The values are carefully chosen in order to correspond with the certain standardized capacities of LTE, IEEE 802.11n and IEEE 802.11ac.

All RATs are constantly attacked by a different kind of DDoS attacks (TCP SYN flood, UDP flood, and ICMP Ping Distributed DoS (DDoS) attacks and jamming attacks). Those DDoS attacks are causing inability to access any service from the MTs and the jamming attacks are preventing the MTs to communicate by occupying the channel that they are communicating. Moreover, in RAT1 (LTE) we have adaptive modulation and coding, i.e., at different destination points from the RAT1 (LTE) base stations we are using different modulation and coding schemes. For mobile nodes physical mobility, we have adopted 2-dimensional implementation of the Gauss-Markov Mobility model considering average speeds in the range of 20-320 km/h. This mobility model provides a high level of randomness for user mobility. Also, when a group of mobile nodes is leaving the RAT1 (macro) cell, it is supposed that the same number of mobile nodes is incoming in the observed cell from other neighboring cells, so the number of mobile nodes per cell remains constant over the simulation time. The multimedia service flow model consists of three types of services as follows:

1st service type: Video conference with a low bit rate (128 kbit/s) and small latency.

2nd service type: Video-streaming with medium bit rate (256 kbit/s) and low propagation time, plus jitter sensitive.

3rd service type: Data service with high bitrate (512 kbit/s) or larger latency, but has requirements for zero packet delivery errors.

During the simulation for a given number of ordinary active mobile users N, each user is randomly assigned to one of the three types of services defined above.

When the users have MT with ASECQUA module within, for each user are randomly assigned all three types of multimedia services. We have done five cases for this scenario:

Case 1: All MTs are enhanced with ASECQUA module with GA optimizations in our three-RAT MT with three interfaces.

Case 2: All MTs are enhanced with ASECQUA module with LP optimization algorithm, instead of having GA. We refer to this kind of MT as MT with LP module (ASECQUA_LP).

Case 3: All MTs are using only RAT1 technology (only LTE interface), without ASECQUA module within.

Case 4: All MTs are using only RAT2 technology (only IEEE 802.16n interface), without ASECQUA module within.

Case 5: All MTs are using only RAT3 technology (only IEEE 802.16ac interface), without ASECQUA module within.

The simulation results regarding the achievable average aggregated throughput (R) are shown in Fig. 4, which provides results on the average throughput (per cell) versus the number of MTs for all five cases.

Table 1
Parameter Values for the RATs

	Position(s) (meter, meter)	**Network Radius (meter)**	**Network Capacity [kbps]**
RAT 1	(0,0)	2100	300000
RAT 2	(0,0), (120,120), (-120,120), (-120,-120), (120, -120), (0, -255), (0, 255)	70	600000
RAT 3	(0,0), (0, 120), (-120, 0), (120,120), (-120,120), (-120,-120), (120, -120)	40	7000000

The average velocity of the MTs is set to 40 km/h and the total simulation time is 120 seconds (according to [53] it is default service duration for getting valuable statistical results from the Security and QoS measurements for any multimedia services). As one can notice, the throughput for our MT, with ASECQUA module, for any number of used MTs, is much higher than the average throughput values in the case when we use only MTs that can access only RAT1 (R_RAT1_MT), or in the case when we use only MTs that access RAT2 (R_RAT2_MT) or RAT3 (R_RAT3_MT).

Comparing the throughput for the R_ASECQUA_LP curve (where the LP is used as OA) and the throughput in the case when GA is used as OA within the ASECQUA module of MT (R_ASECQUA_GA), the MT with LP is achieving the

highest throughput for any number of ME. This indicates that the MT with LP can be used for middle to high traffic congestion scenarios (more than 360 MTs) because gives overall better yields then GA OA.

Furthermore, in Fig. 5 are presented the average multimedia secure access probability ratio per cell (Pm_sec_acc) values for different velocities of the MTs, with 500 MTs and simulation time of 120 seconds. For the first case, when we use MTs with ASECQUA modules with LP algorithm, the average Pm_sec_acc values are higher than the MTs with ASECQUA modules with the GA algorithm for any average speed of MTs. As it was expected, for the first two Cases (with ASECQUA module) the values for Pm_sec_acc are higher than the values obtained for the cases when we used MTs that can access only one RAT. The difference between MTs with ASECQUA module with GA OA and those with LP OA is in range of 0.125 or less for the Pm_sec_acc per cell. In case of higher velocity (when the average velocity of MTs is more than 200 km/h), the preference should be given to LP OA for all cases where this Secure-QoS parameter (Pm_sec_acc) is crucial for the services. Generally, the higher value for Pm_sec_acc further results in lower packet error ratio, higher service availability, reliability and security, as well as in higher aggregated bit rates due to vertical multi-homing, multi-streaming and RAT aggregation. Finally, Fig. 6 depicted the values for Pm_sec_acc per cell versus the number of MTs, when all MTs are moving with an average speed of 50 km/h and simulation time of 120 seconds. For the cases when we use MTs with ASECQUA modules with LP or GA algorithm, the average Pm_sec_acc values are higher than the other cases when the MTs are without ASECQUA modules.

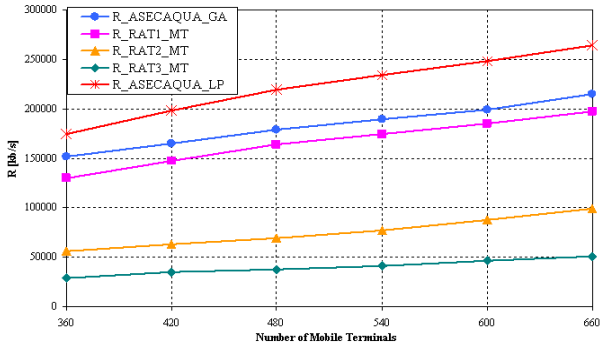

Figure 4
Average throughput per cell versus number of MTs

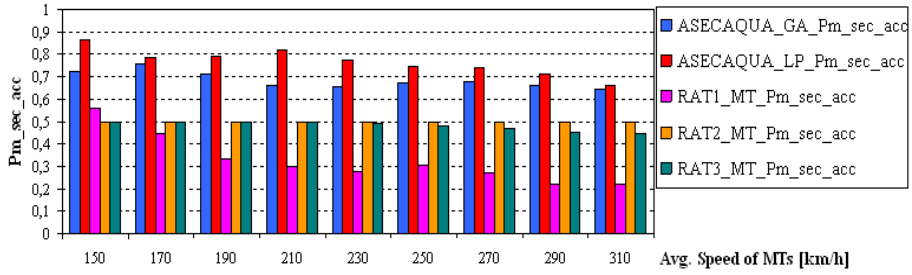

Figure 5

Average Pm_sec_acc per cell versus velocity of MTs

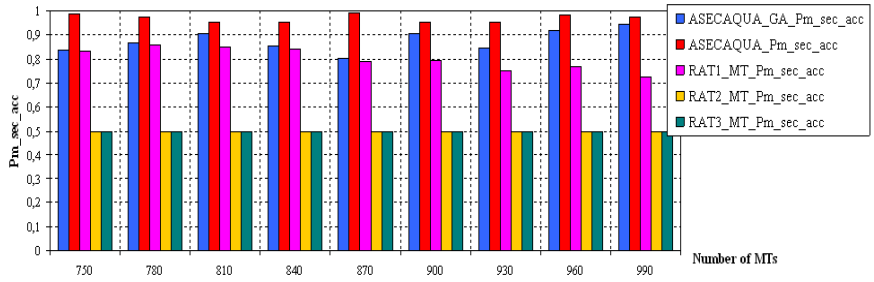

Figure 6

Average Pm_sec_acc per cell versus number of MTs

The difference between those two cases is 0.1 or less in the average multimedia secure access probability ratios. As can be seen, the number of MTs is very high, and this scenario is for dense network conditions.

So, if we have MTs with the ASECQUA module within, with two options for choosing LP or GA optimization algorithms, in those network conditions, where there are high dense networks (where mobile nodes are above hundreds) - we will use LP. However, it is always wise to have a backup and shared combinations of Secure and QoS optimization algorithms for different network conditions and environments. Undoubtedly, the 5G nodes with ASECQUA are achieving superior results regarding the aggregated average aggregated throughput and multimedia secure access probability ratio per service with optimal secure RAT(s) selections.

Conclusions

The trend of integrating criminal and warfare methods with inexpensive technologies to achieve individual, criminal or national security objectives can pose serious challenges to the implementation of future ICT technologies. The expected and promising 5G based technology will not be immune to these threats. Including the jamming process. Solutions that will mitigate the upcoming 5G devices' vulnerabilities from jamming attacks, build trust among the end-users (individuals, corporate, public stakeholders). The presented framework herein

could be adapted to serve corporate or national security purposes. As we have shown, this framework, called the ASECQUA module, can provide future Security and QoS provisioning within the 5G network capacity aggregation with vertical multi-homing and multi-streaming features. The presented results prove that this framework provides the highest level of multimedia, secure access probability ratio and highest aggregated throughputs for each multimedia and broadband service, over secure traffic tunnels. Moreover, the proposed, combined anti-jamming mechanisms, within ASECQUA show results that are almost the same as in the case when no jammer is used. Here we also propose an algorithm for adaptive transmission power and receiver sensitivity control, in order to achieve desired transmission power and receiver sensitivity adjustment. In that manner, optimal, secure and QoS-based usage of available wireless and mobile broadband resources is essential for the excellent provision of any broadband service, with a high level of security.

In one future 5G, a possible scenario for using various broadband services from the end users over the 5G and other heterogeneous wireless and mobile broadband networks, the 5G mobile node and ASECQUA proxy server with vertical multi-homing and multi-streaming security features are able to handle simultaneously multiple RAT connections. Moreover, there will be high speed wireless and mobile connections for each broadband service (e.g., web, video streaming, ftp, etc.) by transmitting each object of each service in a separate IPSec stream, to achieve the highest level of secure communications and satisfied end-users.

Finally, the given advanced framework for 5G and heterogeneous wireless and mobile broadband networks can be one of the key solutions for future network architectures, not only 5G, but beyond. Because of the fact that the presented framework achieves maximal aggregated throughput and multimedia secure access probability ratio, and consequently better overall security and QoS performances. The given advanced framework for 5G could be easy extended for mobile cloud computing and security plus QoS orchestration mechanisms in all network entities, including the smart mobile devices, i.e. the cloud computing would be extended at the edge of the network in a form of intelligent multi-access edge computing. The time is near, where more and more virtual network functionality, including blockchain technology, will be executed in a mobile cloud and edge computing environment, including many parts of our given advanced framework. They together, would provide ubiquitous computing and broadband service to the users, where devices, smart terminals, laptops, machines, but also, smart things and robots would become innovative tools that would produce and use different services and data, i.e. they would be able to provide “Anything as a Service” (AaaS) as well.

References

[1] Federico Boccardi et al.: Five Disruptive Technology Directions for 5G, IEEE Communications Magazine, Vol. 52, No. 2, 2014, pp. 74-80

[2] Naga Bhushan et al.: Network Densification: The Dominant Theme for Wireless Evolution into 5G, IEEE Communications Magazine, Vol. 52, No. 2, 2014, pp. 82-89

[3] Boyd Bangerter, Shilpa Talwar, Reza Arefi, and Ken Stewart: Networks and Devices for the 5G Era, IEEE Communications Magazine, Vol. 52, No. 2, 2014, pp. 90-96

[4] Cheng-Xiang Wang et al.: Cellular Architecture and Key Technologies for 5G Wireless Communication Networks, IEEE Communications Magazine, Vol. 52, No. 2, 2014, pp. 122-130

[5] Toni Janevski: 5G Mobile Phone Concept, IEEE Consumer Communications and Networking Conference (CCNC) 2009, Las Vegas, USA, 2009

[6] Willie W. Lu: An Open Baseband Processing Architecture for Future Mobile Terminals Design, IEEE Wireless Communications, April 2008

[7] Aleksandar Tudzarov and Toni Janevski: Design for 5G Mobile Network Architecture, International Journal of Communication Networks and Information Security, Vol. 3, No. 2, August 2011, pp. 112-123

[8] Josef Noll, Mohammad. M. R Chowdhury: 5G – Service Continuity in Heterogeneous Environments, Wireless Personal Communications, DOI: 10.1007/s11277-010-0077-6, Published online: 31 July 2010

[9] Kris Osbornnov: Samsung works with U.S. military to prototype new high-speed 5G network, Defense Systems, accessed: November 28, 2018 at: https://defensesystems.com/articles/2017/11/02/samsung-5g-halvorsen.aspx

[10] Anirudh Bhagwandas Rathi, Snehal Kalam: 5G Technology and Advancement in Telecommunication at Military Level, Scholars Journal of Engineering and Technology (SJET), 4(1):49-52, 2016

[11] M. Shafi et al.: 5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice, IEEE Journ. Sel. Areas in Commun., Vol. 35, No. 6, Jun. 2017, pp. 1201-1221

[12] R. Kassab, O. Simeone, and P. Popovski: Coexistence of URLLC and eMBB Services in the C-RAN Uplink: An Information-Theoretic Study, in Proc. IEEE Globecom, Abu Dhabi, December 2018

[13] P. Popovski et al.: Ultra-Reliable Low-Latency Communication (URLLC): Principles and building blocks, IEEE Network, Vol. 32, No. 2, Mar. 2018, pp. 16-23

[14] 3GPP: Study on new radio (NR) access technology physical layer aspects, TR 38.802, Mar. 2017

[15] Recommendation ITU-T Y.2052 (02/2008): Framework of multi-homing in IPv6-based NGN

[16] Recommendation ITU-T Y.2056 (08/2011): Framework of vertical multihoming in IPv6-based Next Generation Networks

[17] Next Generation Mobile Network Alliance: 5G White Paper, Version 1.0, Feb 17, 2015

[18] D. Kutscher: It's the network: Towards better security and transport performance in 5G, 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), San Francisco, CA, 2016, pp. 656-661

[19] Ahmad, Ijaz et al.: 5G security: Analysis of threats and solutions. 2017 IEEE Conference on Standards for Communications and Networking (CSCN), 2017, pp. 193-199

[20] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov: Overview of 5G Security Challenges and Solutions, in IEEE Communications Standards Magazine, Vol. 2, No. 1, March 2018, pp. 36-43

[21] SIMalliance: An analysis of the security needs of the 5G market, A SIMalliance 5G Working Group marketing white paper, 2016

[22] Symantec: Internet Security Threat Report, Volume 21, April 2016

[23] P. Schneider and G. Horn: Towards 5G Security, 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, 2015, pp. 1165-1170

[24] M. Hadji-Janev, and Bogdanoski, M.: Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare, Hershey, PA, IGI Global, 2016

[25] A. Risteski, M. Bogdanoski, M. Stoilkovski, M. Jovanovic: Cyber Security Issues of Telecommunication Infrastructure, Chapter, Book: Cyber Security and Resilience Policy Framework, IOS Press, NATO Science for Peace and Security Series - D: Information and Communication Security, September 2014

[26] Ejaz, Waleed et al.: Internet of Things (IoT) in 5G Wireless Communications, IEEE Access. 4. 10310-10314, January 2016

[27] Z. Zhang and S. Li: A Survey of Computational Offloading in Mobile Cloud Computing, 2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Oxford, 2016, doi: 10.1109/MobileCloud.2016.15, pp. 81-82

[28] Singh, S. & Jha, R. K. Jha: A Survey on Software Defined Networking: Architecture for Next Generation Network, Journal of Network and Systems Management, Vol. 25, 321-374, April 2017, https://doi.org/10.1007/s10922-016-9393-9

[29] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov: Security in Software Defined Networks: A Survey, IEEE Communications Surveys Tutorials, Vol. 17, No. 4, Fourthquarter 2015, pp. 2317-2346

[30] Bo Han and al.: Network Function Virtualization: Challenges and Opportunities for Innovations, IEEE Communications Magazine, 53(2), February 2015, pp. 90-97

[31] A. Aissioui, A. Ksentini, A. M. Gueroui and T. Taleb: Toward Elastic Distributed SDN/NFV Controller for 5G Mobile Cloud Management Systems, in IEEE Access, Vol. 3, 2015, pp. 2055-2064

[32] ITU-R: ITU-R M. - Minimum requirements related to technical performance for IMT- 2020 radio interface(s), Report ITU-R M.2410-0, Nov. 2017

[33] ITU Recommendation Y.3101: Requirements of the IMT-2020 network, January 2018

[34] Qualcomm: Accelerating the 5G ecosystem expansion today with LTE Advanced Pro, May 2018. <available link> https://www.qualcomm.com/invention/5g/lte-advanced-pro

[35] Liu, Z., Liu, H., Xu, W., and Chen, Y.: Exploiting jamming-caused neighbor changes for jammer localization, Parallel and Distributed Systems, IEEE Transactions on, 23(3), 2012, pp. 547-555

[36] Wilhelm M., Martinovic I., Schmitt J. B., and Lenders V. Short paper: reactive jamming in wireless networks: how realistic is the threat?. In Proceedings of the fourth ACM conference on Wireless network security (WiSec '11) 2011, ACM, 47-52. DOI=10.1145/1998412.1998422

[37] Chaturvedi P., Gupta K.: Detection and Prevention of various types of Jamming Attacks in Wireless Networks, IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501, Vol. 3, No. 2, April 2013

[38] Xu, W., Trappe, W., Zhang, Y. & Wood, T.: The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks, In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, ACM MOBIHOC, 2005, pp. 4657

[39] Acharya, M., Sharma T., Thuente, D., and Sizemore, D.: Intelligent jamming in 802.11b wireless networks, In Proceedings of OPNETWORK-2004 Conference, Washington D.C., USA, 2004

[40] Mitko Bogdanoski, Aleksandar Risteski, Pero Latkoski, Tomislav Shuminoski: Power Control as an Effective Method Against Low Power Jamming, CICSyN2014, Tetovo, Republic of Macedonia, May 27-29, 2014

[41] Khan, S., Loo, K. K., Naeem, T. and Khan, M. A.: Denial of Service Attacks and Challenges in Broadband Wireless Networks, IJCSNS International Journal of Computer Science and Network Security, 2008

[42] Acharya, M. and Thuente, D.: Intelligent Jamming Attacks, Counterattacks and (Counter)2 Attacks in 802.11b Wireless Networks, In Proceedings of the OPNETWORK-2005 Conference, Washington DC, USA, August 2005

[43] Tomislav Shuminoski, Toni Janevski: Radio Network Aggregation for 5G Mobile Terminals in Heterogeneous Wireless and Mobile Networks, Wireless Personal Communications, Vol. 78, Issue 2, 2014, pp. 1211-1229

[44] T. Shuminoski, T. Janevski: 5G mobile terminals with advanced QoS-based user-centric aggregation (AQUA) for heterogeneous wireless and mobile networks, Wireless Networks, 22(5), July 2016, pp. 1553-1570

[45] Tomislav Shuminoski, Toni Janevski, Aleksandar Risteski and Mitko Bogdanoski: Security and QoS framework for 5G and Next Generation Mobile Broadband Networks, IEEE EUROCON 2017, Ohrid, Macedonia, 6-8 July 2017

[46] IEEE 802.11h Standard, Part 11: Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications, Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe, December 2003

[47] Mitko Bogdanoski, Aleksandar Risteski: Wireless Network Behavior under ICMP Ping Flood DoS Attack and Mitigation Techniques, International Journal of Communication Networks and Information Security (IJCNIS), Vol. 3, No. 1, 2011

[48] Mitko Bogdanoski, Tomislav Shuminoski, Aleksandar Risteski: Analysis of the SYN Flood DoS Attack, International Journal of Computer Network and Information Security, Vol. 5, No. 8, June 2013, pp. 1-11

[49] Mitko Bogdanoski, Aleksandar Toshevski, Dimitar Bogatinov, and Marjan Bogdanoski: A novel approach for mitigating the effects of the TCP SYN flood DDoS attacks, World Journal of Modelling and Simulation, 12 (3), 2016, pp. 217-230

[50] Boris Mihajlov, Mitko Bogdanoski: Analysis of the WSN MAC Protocols under Jamming DoS Attack, International Journal of Network Security, Vol. 16, No. 4, July 2014, pp. 304-312

[51] Mitko Bogdanoski, Pero Latkoski, and Aleksandar Risteski: Analysis of the Impact of AuthRF and AssRF Attacks on IEEE 802.11e-based Access Point, Mobile Networks and Applications, Volume 22, Issue 5, October 2017, pp. 834-843

[52] Peco Stojanoski, Mitko Bogdanoski, Aleksandar Risteski: Wireless Local Area Network Behavior under RTS flood DoS attack, 20th

Telecommunications Forum TELFOR 2012, IEEE Conference, 20-22 November 2012

[53] Recommendation ITU-T E.804 (02/2014): QoS aspects for popular services in mobile networks