Novel Model of Adaptive Module for Security and QoS Provisioning in Wireless Heterogeneous Networks

Mitko Bogdanoski[1], Tomislav Šuminoski[2], Aleksandar Risteski[3], Toni Janevski[4]

[1]Military Academy "gen. Mihailo Apostolski", 1000 Skopje, Republic of Macedonia, mitko.bogdanoski@morm.gov.mk[1]
[2,3,4] University "Sv. Kiril I Metodij", Faculty of Electrical Engineering and Information Technologies, Karpos 2 bb, 1000 Skopje, Republic of Macedonia, {tomish, acerist, tonij}@feit.ukim.edu.mk[2,3,4].

***Abstract* – Considering the fact that Security and Quality-Of-Service (QoS) provisioning for multimedia traffic in Wireless Heterogeneous Networks are becoming increasingly important objectives, in this paper we are introducing a novel adaptive Security and QoS framework. This framework is planned to be implemented in integrated network architecture (UMTS, WiMAX and WLAN). The aim of our novel framework is presenting a new module that shall provide the best QoS provisioning and secure communication for a given service using one or more wireless technologies in a given time.**

***Keywords* – Adaptive, Cross-Layer, Security, Triple-mode, Quality-of-Service (QoS).**

1. INTRODUCTION

The Security issues and Quality of Service provisioning in the nowadays and future wireless mobile networks are becoming increasingly important objectives. The reason for these is the fact that those networks are vulnerable on different kind of attacks and in the same time are promising to provide a broad range of multimedia services to mobile users, with enormous spectrum of advanced capabilities and high security level in the communication. The implementation of many advance capabilities, such as: ubiquitous mobility, enormous processing power of the mobile equipment (ME), adaptive high-level QoS support, high security level and etc., require great thoughtfulness, scalability and thorough full analysis. Since radio bandwidth is one of the most precious resources in the wireless mobile heterogeneous systems and in the same time the most vulnerable of attacks, joint efficient adaptive Security and QoS (SQoS) framework is very important to guarantee SQoS for any given services and to maximize radio resource utilization simultaneously. Moreover, the most significant SQoS parameters in the existing (and future) wireless heterogeneous networks are the throughput, packet delivery ratio, packet error ratio, call blocking probability, delay and jitter (especially when we use real-time services).

In the next generation mobile and wireless network, which is seen as user-centric concept instead of operator-centric as in 3G or service-centric concept as seen for 4G, the mobile user is on the top of all [1]. The MEs will have access to different wireless technologies at the same time and they should be able to combine different flows from different technologies using adaptive SQoS algorithms. Furthermore, each wireless and mobile network will be responsible for handling user-mobility, while the mobile terminal will make the final choice among different wireless and mobile access network providers for a given service. In that context, satisfied QoS provisioning for wireless and mobile multimedia networks, together with high level of secure communication, are increasingly becoming crucial targets.

Moreover, the analysis in this paper is focused on adaptive SQoS framework for multimedia (real-time and non-real-time) services over integrated UMTS, WiMAX and WLAN networks. This framework is considered in a loose coupling architecture, using novel advanced triple-mode ME node with adaptive intelligent SQoS module within.

Today, the UMTS network can support services with maximum data rate of several Mbps and it has an advantage when referring to voice and soft handover of the voice. On the other hand, WiMAX, based on the OFDMA (Ortogonal Frequancy Division Multiple Access) technique, is offering higher data rates, better performance (considering multipath tolerance, interference rejection and spectral efficiency), high QoS support (symmetric link and data oriented MAC, and lower costs. The new mobile WiMAX standard, 802.16m, is expected to offer high speed mobility support and data rates support of 1Gbps for fixed stations and 100Mbps for mobile stations. Furthermore, the IEEE 802.11a and IEEE 802.11g can provide up to 54 Mb/s in 5GHz and 2.4GHz bands, respectively. Also, 802.11n can go up to several hundreds Mbps. However, WLAN, compared to UMTS and WIMAX base stations, is

lacking support for user mobility and has significantly smaller coverage areas by access points (AP). Such complimentary characteristics of these three popular technologies have stimulated research efforts to integrate 3G, WiMAX and WLAN networks, so that MEs can choose the network that has better network quality when they are covered by all of these networks and can have continuous services when they roam in the integrated network environment.

The hardware requirement for integrating UMTS, WiMAX and WLAN networks is to build triple-mode ME (already exist only dual-mode ME) with integrated adaptive SQoS module (novel framework in this field which can find crucial place in next generation mobile and wireless equipment). This module will have capability of accessing these three networks and choose the best connection according to SQoS requirements for the given service, and roam between the networks as many times as needed by using vertical handovers executed by the ME. The prerequisite for this is ME to have Service Level Agreements (SLA) with all three networks. The reason for this is that all these networks can belong to different network providers.

Without loss of generality, this adaptive SQoS Cross-layer IP (SQoSXIP) framework can be used in any mobile and wireless IP multimedia networks. Nowadays many types of ME have already integrated WLAN and Bluetooth interfaces, and in the near future many MEs, besides their UMTS, WLAN, WiMAX, Bluetooth, ZigBee, WPAN etc. radio interfaces, will also have Long Term Evolution (LTE) interfaces. However, when there are different wireless and mobile networks on one side, and single ME on the other, then consequently the user of that ME should have possibility to use all those technologies in the range using his/her personal settings in the ME, or this user can choose only one from all available technologies. For that purpose the Open Wireless Architecture (OWA) [2] is proposed to provide open baseband processing modules with open interface parameters for supporting different wireless and mobile communication technologies. The main mobile phone design concept as well as protocol stack for this approach is introduced in [1].

The remainder of this article is structured as follows. Section 2 gives an overview of the most relevant research works in this field. In Section 3 the system model and algorithms are described. In Section 4 the example of possible implementation of our module. Finally, Section 5 concludes this paper.

2. RELATED WORKS

The interest for adaptive SQoS provisioning is growing together with the tremendous development of adaptive multimedia services in mobile and wireless communication networks, where it is possible to increase or decrease the bandwidth of individual ongoing flows.

When we focus on architectures for integrated heterogeneous networks, i.e. WLAN and UMTS systems, they can be grouped into two categories based on the independence between the two networks [3], tight coupling and loose coupling. The loose coupling architecture enables the two networks to be deployed independently, but it results in poor QoS provisioning (longer delays for signaling and vertical handovers). Furthermore, schemes for dual-mode ME for UMTS/WLAN interworking network have been proposed in [4] and [5], but without emphasized QoS issues. Similar on previous dual-mode ME node for UMTS/WLAN, in [6] is presented advanced one, with implemented handover logic modules within. The dual-mode UE design includes a monitoring and reporting unit to determine the status of the interfaces and an interface selection unit to activate or deactivate the interfaces (UMTS and WLAN) for mobile handoff. The results indicate a smoother and seamless handoff process. The lack of this model is in focusing only in mobile HO processes and not implementing any adaptive QoS framework for improving the results of other QoS parameters. Similar to our work in [7] the adaptive wireless end-to-end QoS algorithm is presented, but with dual-mode ME. That algorithm solves the main QoS problems (congestion, wireless medium, handovers, temporary disconnecting and ect.) within the Network Layer in integrated WLAN/UMTS Networks. However, the lack of the adaptive QoS framework presented in [7] is the focus only in video streaming delivery (real-time services) over heterogeneous networks.

In addition to the QoS parameters, there are also plenty of researches considering security issues as well, with the main objective of increasing the security level during vertical handover, and consequently to that, increasing the QoS. The authors of [8] propose a new architectural view and methodologies for QoS and security support in 4G networks. Actually, they present an architecture for **Sea**mless Mobility with **S**ecurity and Q**oS** Support (SeaSoS), that integrates mobility schemes with QoS and security measures, and discuss the main issues toward realizing this architecture. With their efficient propose of integration both user applications' QoS requirements and achieve efficient authentication, authorization and key exchange are guaranteed. Furthermore, the authors of [9] modifying the EAP-AKA keying framework propose an improved authentication scheme. The improved scheme enables a WLAN user to efficiently access packet switch services through the 3G networks. Furthermore, the user can use the new keying framework efficiently for realizing the future re-authentications and handover authentications. Using OPNET simulation it is proved that the proposed scheme can reduce authentication latency significantly. The novel AAA (Authentication, Authorization and Accounting) architecture proposed in [10] is supporting policy-based negotiation for establishing spontaneous roaming agreements in heterogeneous networks. For

spontaneous and dynamic roaming agreements and interworking to be done a new proposed architecture integrates policy-based negotiation into the normal user association and authentication process. Furthermore, the authors designed a new Diameter application to handle the negotiation for spontaneous roaming agreement, and we also designed policy language and policy based negotiation process. The proposed integration model minimizes changes to existing AAA architecture for enabling the new paradigm of automated provider interworking and cooperation. In [11] a solution which involves single sign-on authentication is proposed. This mechanism allows the end user to roam between different administrative domains and access network technologies. In the proposed solution a number of authentication protocols (as well as an EAP-SIM server) are integrated and does not require any end-user interactions while roaming, thus enabling a seamless roaming experience. We describe a prototype implementation of this solution using GPRS/UMTS/WLAN networks and present our conclusions using measurements on this prototype. The authors of [12] showed how the new communications architecture for heterogeneous networking called Y-Comm can have a multi-layer security framework. Their approach proposes a four-layer security integrated module to protect data and three targeted security models to protect different network entities, thus providing security in different situations without affecting the dynamics of the 4G networks. The AAA handling solution proposed by the authors of [13] is based on the using of common database for storing user information. Regardless of the selected access technology, the authors propose using of user@realm identities for AAA. Actually, they are introducing a new function in which port-based network access control is used in combination with DHCP mechanisms for IP address allocation, at which way, the PPP-based and the Ethernet-based access technologies are handled uniformly. Furthermore, in this papaer the problems around inter domain mobility and the neediness for trust relationships between service providers are also discussed.

The main motivation that led us to develop novel adaptive SQoS module, which will provide intelligent high level of QoS in any wireless and mobile heterogeneous network (including integrated UMTS/WLAN networks, as in [14]) and appropriate security level, using every available technology at same time, are taken from [1]. To emphasize that compared with other related works, our adaptive SQoS module is implemented on IP level. Moreover, in some previous works in this field (with the first version of only adaptive QoS module) there are early simulation results and analysis for adaptive QoS VoIP provisioning (real-time services) in integrated WLAN/UMTS networks [15] and also, adaptive QoS provisioning for non-real time services in heterogeneous wireless networks [16]. After improvements of that Adaptive QoS Module within the ME, we expecting even superior results then the previous one, and even better SQoS provisioning in heterogeneous wireless and mobile networks. Furthermore, in the next section the intelligence of our novel adaptive SQoS module is elaborated.

3. SYSTEM MODEL AND ALGORITHM

The main position of our novel SQoSXIP module within ME triple-mode node is illustrated in Figure 1. As can be seen, our novel ME is triple-mode with three interfaces: WiMAX, UMTS and WLAN and with Adaptive SQoS module within IP layer. According to [1] and [2], physical and OWA define the wireless technology. Without doubts, the network layer will be IP, but separation of this layer into two sub-layers will be necessary. The Upper IP Network Layer has one unified IP address within, and is nominated for routing as well as for creation of sockets to the upper application layer. The other sub-layer, Lower IP Network Layer may include several different IPv4 (or IPv6 addresses), one IP address for each of the three radio interfaces, while each of these IP addresses will be mapped with unified IP address of the Upper IP Network Layer. In the middleware between the Upper and Lower IP Network layers will be address translation module, which shall maintain and translate IP addresses from Upper IP Network address (one IPv4/IPv6) to different Lower IP Network layer IP addresses (IPv4 or IPv6), and vice versa.

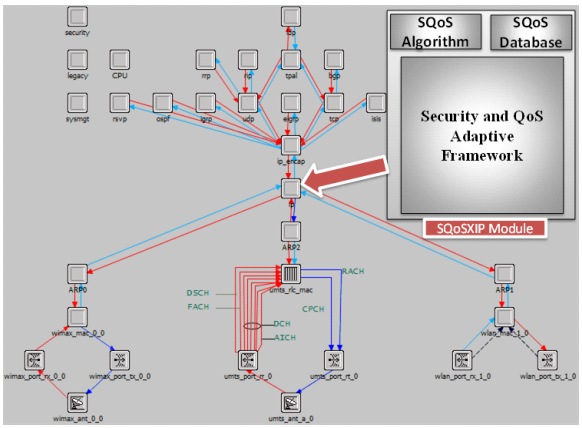

Fig. 1 – Triple-Mode SQoSXIP Module within ME

The core of our work is development of novel adaptive SQoS Cross-layer IP Module; we will refer to it as SQoSXIP, which is defined separately from each wireless technology (e.g. UMTS, WLAN, WiMAX, 3G-LTE, 4G, etc.). It is implemented on IP Network Layer, which will be able to provide intelligent SQoS management and routing over variety of network technologies. Moreover, the SQoSXIP module is able to combine simultaneously several different traffic flows transmitted over the same or different wireless access interfaces, achieving higher throughput and optimally using the radio resources. Furthermore, on Fig. 2 the algorithm within SQoSXIP module can be seen.

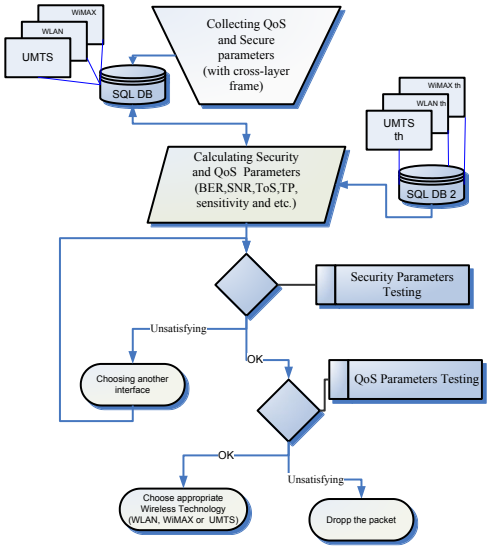

Fig. 2 – Illustration of SQoSXIP Module algorithm

For the purpose of the SQoSXIP, the ME must collect SQoS parameters, such as delay, jitter, losses, bandwidth, reliability, Packer-Error-Ratio (PER), Signal-to-Noice-Ratio (SNR), Transmission Power (TP), sensitivity etc., continuously, at given time intervals (all the time while simulation is going on), by collecting the measurements data via cross-layer packet formats (special C++ code developed in OPNET Modeler [17] for cross-layer communication) from OSI layer 1 up to IP Network layer, and then storing the data into three-dimensional matrix variable within the SQoSXIP module. This three-dimensional matrix is a small SQoS DB (database), which can be easy extended, in a more complex multi-dimensional matrix (more complex DB, which will save all other relevant parameters for any used mobile wireless technology). The first row of this matrix contains WiMAX SQoS parameters, second row contains UMTS SQoS parameters and the third row contains the WLAN SQoS parameters, appropriately. On the other hand, with one cross-layer frame, for each send packet, the Type-Of-Service information (ToS field in IPv4 or DSCP field in IPv6) from Application Layer is collected (from the arriving/departuring packets), in order to implement packet scheduling priority, i.e. higher priority for real-time service packets (VoIP, Video-conference, VoD and etc.). Before every downlink transmission of IP packet from SQoSXIP down to UMTS, WiMAX or WLAN MAC modules, the SQoSXIP module is doing service quality and security analysis. This analysis is done using the data stored in the SQoS DB in the IP Network Layer of ME for given time period in the past (e.g., seconds, minutes) in order to choose the best wireless connection upon required QoS and under reliable (secure) channel.

Here, in our current implementation, we can test only: ToS, SNR, PER, TP, sensitivity level, CPU usage, energy consumption, number of control messages, which are collected from Application and OWA Layer (OSI Layer 1 and OSI Layer 2) via cross-layer frames (in OPNET modeler this C++ class we called XMessage, which saves previous mentioned parameters in privet variables). When the IP packet comes to the SQoSXIP module, it always fist try to get admission (in downlink) to the WLAN whenever it is available (i.e. all tested WLAN parameters are above their appropriate WLAN thresholds and moreover, the WLAN utility function in [4] given with equation (8), is satisfied). Second, if SQoSXIP module doesn't get WLAN admission, it tries to get admission to the UMTS network (all tested UMTS parameters are above their appropriate UMTS thresholds and also the UMTS utility function given in [4] (equation (7)) is satisfied) and in the end SQoSXIP module try to get admission on WiMAX network.

Finally, SQoSXIP module sends the packet that comes from IP Network Layer down to the chosen LL/MAC module via appropriate IP Network Layer or drops it in the case when there is no admission to any of the given wireless mobile networks. However, every packet goes through packet priority scheduling, before it is passed to the above mentioned downlink procedure.

On the other hand, in uplink, all packets which are coming from all LL/MAC modules are received in Upper Network Layer, and send from SQoSXIP module to Transport Layer without any losses up. With those procedures different flow combining is done within the SQoSXIP module.

4. IMPLEMENTATION IN NETWORK INTEGRATED ARCHITECTURE

In order to achieve more compact performance outline for our SQoSXIP algorithm, and to inspect its behavior under different circumstances (considering the QoS and security issues) we are going to use OPNET Modeler simulator.

General example of heterogeneous wireless network which considers integrated networks (UMTS, WiMAX and WLAN) and proposed ME is shown on Fig.3.

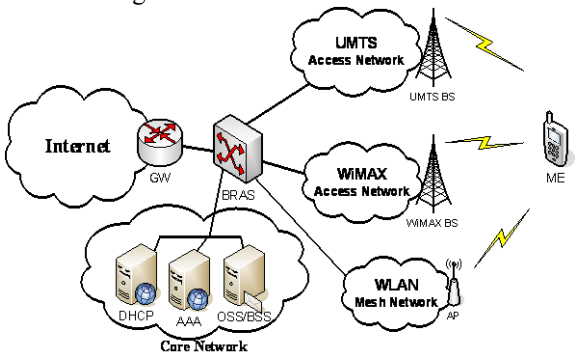

Fig. 3 - Simple scenario for ME with SQoSXIP algorithm within.

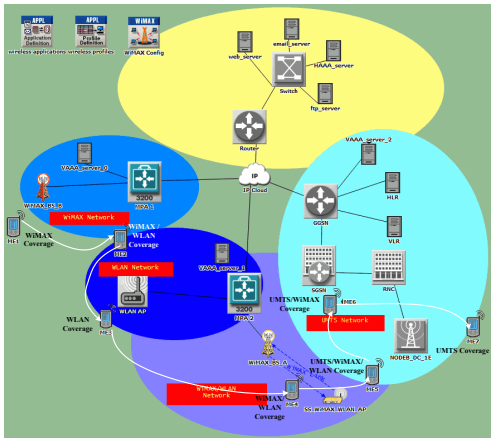

Fig. 4 - Integrated heterogeneous scenario

The integrated heterogeneous network architecture composed using OPNET Modeler is shown in Fig. 4. This architecture includes 5 domains: (1) WLAN domain, (2) UMTS Domain, (3) WiMAX Domain, (4) WiMAX/WLAN Domain, (5) Home Network Domain. (1) **The WLAN domain** is composed of a Visiting AAA server (VAAA), access points (APs) and a WLAN Router (in our case MPA (Mobility Proxy Agent)) that is a gateway to Home Network. (2) **The UMTS domain** includes some core network elements such as the Gateway GPRS Support Node (GGSN), the serving GPRS support node (SGSN), a VAAA server and the Home Location Register (HLR) and Visitor Location Register (VLR). It also includes Node BS (Base Station) and a RNC (Radio Network Controller). Through this domain, the 3G user can access the 3G core networks. (3) **The WiMAX domain** generally includes AAA server (VAAA), WiMAX BS and WiMAX Router (MPA) as a gateway to the Home Network. (4) **The WiMAX/WLAN domain** which includes WiMAX BS, WiMAX/WLAN router, AAA server (VAAA) and Switch (MPA) to connect it to the Home Network. (5) **The Home Network domain** along with the other servers (email, web, ftp etc.) consists of a Home AAA server (HAAA). The HAAA server retrieves authentication information from the Home Subscriber Service (HSS)/Authentication Centre (AuC) and validates authentication credentials provided by users. In this domain there is also a router which is gateway to the different integrated networks.

During our work regarding this project several different scenarios will be examined: First scenario is when the ME is covered by all three networks; Second scenario is when the ME is covered by UMTS and WiMAX networks; Third scenario is when the ME is covered by UMTS and WLAN networks and; Forth scenario when the ME is covered by WiMAX and WLAN networks.

If we compare our model with traditional networks model, it is easily apparent that this network, due to its heterogeneous nature and the complexity of the deployed architecture model, raises security concerns. Some of the concerns, such as the initial access authentication, have been paid a lot of attentions by researchers. On the other hand, some of the major security concerns, especially the authentication during handover, are neglected by released specifications about this technologies and previous contributions; even it is obvious that these concerns are very important for the successful deployment of the interworking networks and the provision of high users QoS.

The standard AAA architecture for integrated network (in our case UMTS, WLAN and WiMAX) is EAP with backend Radius or Diameter AAA server. In order to improve the security architecture for heterogeneous networks during vertical handover we are using EAP/Diameter authentication procedures, shown on Fig 5. The messages defined by the EAP method are sent from the mobile station to an authenticator. The authenticator (AP/BS) then forwards the messages to the authentication server (VAAA) using either the radius or diameter protocols [18]. In our case we are using diameter protocol due to many advantages over radius protocol [19]. VAAA does initiate ME details request to home network AAA server (HAAA) by identifying the NAI of the user ID for authentication. HAAA collects data associated to user ID from request and reply message to HA and sends back reply to VAAA. VAAA server sends mobility registration request to MPA (Mobility Proxy Agent) of network associated to the AP with collected details from HAAA. MPA does registration with HA using details from AAA server, and sends acknowledgement to AAA server. After authenticating user terminal and upon receiving the reply from MPA, visiting AAA server send success with the IP address of the ME sent by the home AAA server to AP/BS.

During our work regarding this concept, along with QoS measurements and improvement, we are going to consider behaviour of the proposed SQoSXIP module under the different types of attacks, especially different deauthentication and flooding (TCP, UDP, ICMP Ping, Jamming) attacks. The results we are going to get from different simulation scenarios will be used for improvement of security mechanisms used within SQoSXIP module.

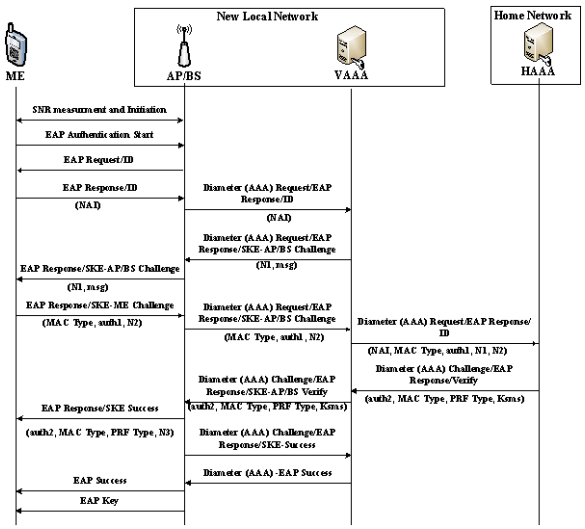

Fig.5 Message flow during vertical handover scenario

5. CONCLUSION

In this paper, a step forward is made with introducing a new adaptive SQoS framework in heterogeneous wireless and mobile network, using triple-mode WiMAX/UMTS/WLAN mobile terminals.

According to the analysis, our proposed next generation triple-stack WiMAX/UMTS/WLAN ME with adaptive SQoSXIP module should perform fairly well under a variety of network conditions regarding: user mobility, background traffic load and number of nodes, interfaces, and various attacks; achieving overall better performances in comparison with the cases when only WLAN, WiMAX or UMTS MEs have been used respectively. The presented logic of SQoSXIP module in the triple network scenario, can be easily generalized in multi wireless networks scenario, including any wireless NGN access network.

In our future work we are focusing on development and implementing such a SQoSXIP module, by using OPNET modeler, in different simulation scenarios with additional network conditions as inputs for intelligent wireless access decisions. Some of the additional network conditions during our work will be simulating of different attacks against different integrated wireless networks and ME respectively. Moreover, we plan to add Bluetooth and LTE interfaces in OWA Layer, and use more complex algorithm in SQoSXIP module, together with more complex database. This advanced SQoSXIP module should be able to choose the best wireless technology under given QoS requirements and security conditions and time intervals, for best SQoS satisfaction. Also, it can combine different traffic flows from or to different heterogeneous wireless and mobile networks, with aim of achieving superior QoS provisioning (i.e., maximal throughput, minimal delay and jitter, maximal PDR, minimal packet error, minimal CPU usage, minimal energy consumption etc.). All given capabilities and analysis of our novel adaptive SQoS framework are fundamental parts of the next generation mobile and wireless network paradigm.

6. REFERENCES

[1] T. Janevski, “5G Mobile Phone Concept” – CCNC conference in Las Vegas, 2009.

[2] W. W. Lu, “An Open Baseband Processing Architecture for Future Mobile Terminals Design”, IEEE Wireless Communications, April 2008.

[3] M. Buddhikot, G. Chandranmenon, S. Han, Y. W. Lee, S. Miller and L. Salgarelli, Integration of 802.11 and Third-Generation Wireless Data Networks, Proc. IEEE INFOCOM, Apr. 2003.

[4] Y. Zhou, Y. Rong, H.-A. Choi, J.-H. Kim, J. K. Sohn, and H. I. Choi,"A Dual-Mode Mobile Station Modules for WLAN/UMTS Internetworking Systems," Proc. OPNETWORK 2007, Washington, DC, August 27-31, 2007.

[5] Nicola Baldo, Federico Maguolo, Marco Miozzo, Michele Rossi, Michele Zorzi, ”Ns2-MIRACLE:a Modular Framework for Multi-Technology and Cross-Layer Support in Network Simulator 2”, NSTools ’07, October 22, 2007, Nantes, France.

[6] A. A. Al-Helali, A. Mahmoud, T. Al-Kharobi, T.Sheltami, "Simulation Of a Novel Dual-Mode User Equipment Design For B3G Networks Using OPNET", Third International Conference on Modeling, Simulation and Applied Optimization Sharjah,U.A.E, January 20-22 2009.

[7] O. B. Karimi, M. Fathy, "Adaptive end-to-end QoS for multimedia over heterogeneous wireless networks", Computers & Electrical Engineering (CEE) 36(1):45-55, 2010.

[8] X. Fu1, D. Hogrefe1, S. Narayanan, R. Soltwisch, “QoS and Security in 4G Networks”, First Annual Global Mobile Congress, Shanghai, China, October 2004.

[9] X. Li, X. Lu, J. Ma, Z. Zhu, L. Xu and Y. H. Park, “Authentications and Key Management in 3G-WLAN Interworking”, Mobile Networks and Applications, Springer, July 2010.

[10] J. Fu, M. Shin, J. C. Strassner, N. Jain, V. Ram, S. Upadhyaya, and W. Arbaugh, “AAA for Spontaneous Roaming Agreements In Heterogeneous Wireless Networks”, Autonomic and Trusted Computing 2007, Hong Kong, China.

[11] M. Živković, M. M. Buddhikot, K. Lagerberg, “Jeroen van Bemmel[1]Authentication across heterogeneous networks”, Bell Labs Technical Journal, Summer 2005

[12] G. Mapp, M. Aiash, A. Lasebae, R. Phan, “Security models for heterogeneous networking”, Proceedings of the 2010 International Conference on Security and Cryptography (SECRYPT), July 2010

[13] D. Granlund, K. Andersson, M. Elkotob, C. Åhlund, “A uniform AAA handling scheme for heterogeneous networking environments”, 3rd IEEE LCN Workshop on User MObility and VEhicular Networks (ON-MOVE 2009) Zürich, Switzerland; 20-23 October 2009

[14] W. Song, H. Jiang, W. Zhuang “Performance analysis of the WLAN-First scheme in Cellular/WLAN interworking”, IEEE transactions on wireless communications, Vol.6, Issue 5, pp.: 1932-1952, May, 2007.

[15] T. Shuminoski, T. Janevski, "Novel Adaptive VoIP QoS Provisioning In Integrated UMTS/WLAN Networks", ICEST 2010, Ohrid, Macedonia, 23-26 June, 2010.

[16] T. Shuminoski, T. Janevski, "Adaptive QoS Provisioning for Non-real Time Services in Heterogeneous Wireless Networks", TELFOR 2010, 18-th Telecommunications Forum, Belgrade, Serbia, November, 2010.

[17] OPNET Documentation

[18] M. Bogdanoski, P. Latkoski, A. Risteski, B. Popovski “IEEE 802.16 Security Issues: A Survey”, 16th telecommunication forum TELFOR 2008.

[19] M. Bogdanoski, P. Latkoski, T. Šuminovski, A. Risteski, “Authentication, Authorization and Accounting Provided by Diameter Protocol”, An ETAI-IFAC Multi-Conference, ETAI/AAS/DECOM 2009, Ohrid, 2009.