The 9th International Conference on Business Information Security (BISEC-2017), 18th October 2017, Belgrade, Serbia

PERFORMANCE PREDICTION IN SECURE TELECOMMUNICATION SYSTEM WITH QUALITY OF SERVICE GUARANTEES

STOYAN PORYAZOV
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, stoyan@math.bas.bg

DMYTRO PROGONOV
Institute of Physics and Technology, National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", d.progonov@kpi.ua

EMILIYA SARANOVA
University of Telecommunications and Posts, Sofia, Bulgaria,
Institute of Mathematics and Informatics, BAS, emiliya@cc.bas.bg

ZLATOGOR MINCHEV
Institute of ICT, Bulgarian Academy of Sciences, zlatogor@bas.bg

Abstract: *This paper explores a model of overall telecommunication systems, including users, terminals, and a network with Quality of Service (QoS) guaranties. Apart from GSM, BSDN and others, generalized virtual networks (VNET) with overall QoS guaranties have been considered also. In our approach, the network traffic, terminal traffic for A (calling) and B (called) terminals and users' traffic have been divided and considered separately, in their interrelationship.*

The conceptual model consists of a limited number of homogeneous terminals and users' behavior parameters, including repeated calls. The call attempt losses, considered in every service stage, are generalized.

In most cases, information transmitted between communication parties is accessible for third parties. For counteraction against channel eavesdropping in special-purpose communication systems, like commercial and governmental e-mail services, military systems, additional security communication layer is used. This layer is responsible for establishing the core secure communications services, such as cipher keys distributions, message authentication, integrity controlling etc.

We extend the generalized conceptual model, of the considered telecommunication systems, by including the information protection stage, which can be activated on-demand. This stage may include hardware and software components and may cause additional delay and distortions.

The analytical model worked out, allows estimation of the influence of the security stage on the communication systems performance as well as prediction of the overall systems' QoS. The results obtained are a base for further QoS and Quality of Experience (QoE) management models.

Keywords: *Overall Telecommunication System and Network Performance, Information Protection, Quality of Service Guaranties*

1. INTRODUCTION

Our main objective is development of scalable conceptual and analytical performance models of overall telecommunication systems, allowing prediction of the values of many Quality of Services (QoS) indicators as functions of user's , network's and service's behavior

The importance of the teletraffic models, particularly of the overall QoS indicators, for Quality of Experience assessment is emphasized by Fiedler [1].

The network traffic indicators, in force [2] are not suitable for overall telecommunication system, including users. Users are shown in "Schematic contributions to end-to-end QoS" in [3], but they are not connected to the network.

The influence of the security services on the overall QoS parameters in the telecommunication systems is not considered in the available publications, due to the complexity of the problem.

In the present paper Information Security Stage (ISS) Concept is added and integrated in the Overall Telecommunication System Model [4]

2. BASE VIRTUAL DEVICES LEVEL.

In the bottom of the structural model presentation, we consider "base virtual device", which does not contain other virtual devise, in the conceptual model considered.

In the bottom of the structural model presentation, we consider "base virtual device", which does not contain other virtual devise, in the conceptual model considered.

A base virtual device has the following graphic presentation and notation of its parameters:

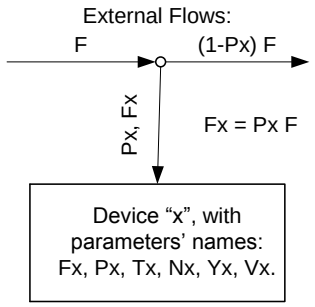

Fig. 1. Graphic presentation of a Base virtual device, named "x" and its parameters' names.

Parameter Names. Parameter Names denotations, connected with one base virtual device are (for terms definition see [5]: F – Frequency (intensity of incoming rate) of the flow of requests (requests per time unit); P – Probability of direction of the requests towards the device considered; T – Time duration of the service of a request in the device considered; Y – Traffic Intensity (Erlang).

Functional Normalization. In our models we consider monofunctional idealized base virtual devices, of the following types (Fig. 1):

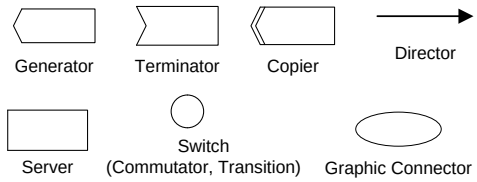

Fig. 2. Graphic block presentation of the main virtual base mono-functional devices used.

Parameters' Qualification. Traffic qualification is necessary and it is used in [5] but without any attempt for including the qualifiers in the parameters' names. Since 2006 [6] we use up to two qualifiers as a part of the parameter's name, which are used for parameters characterization

3. SERVICE PHASE

For more precise traffic characterization, in a pool of resources, we propose [4] the following definitions:

Definition 1: Served traffic in a pool of resources, is traffic, occupying (using) resources of the pool.

Definition 2: Carried traffic in a pool of resources, is successfully (effectively, completed) served traffic in the pool.

Definition 3: Parasitic traffic in a pool of resources is unsuccessfully (not effectively, not completed) served traffic. Parasitic traffic uses real resources, but not for an effective service.

In definitions 1 and 2 served and carried traffics are different, despite the ITU-T definition: "traffic carried: The traffic served by a pool of resources" ([5], Term 5.5).

4. CAUSAL GENERALIZATION

In this paper causal generalization is proposed, as an aggregation of all unsuccessful (parasitic) service cases (*prs.Ys*), from one hand, and all successful (carried (*crr.Ys*)), from the other hand.

By definition, served traffic is a sum of the parasitic and carried traffic: *srv.Ys = prs.Ys+crr.Ys.*

5. SERVICE STAGE CONCEPT

Service Stage is a service presentation containing: one service phase, realizing a function of the service; all auxiliary service phases, directly supporting the function realization, but are not parts of the function.

The intensity of the flow of offered to the stage 'g' call attempts is *ofr.Fg*, of the outgoing carried flow is *crr.Fg*, and of the parasitic served calls is *prs.Fg*.

For every service stage 'g' in the telecom system considered, we will use the following QoS indicator (*Qg*):

$$Qg = \frac{crr.Fg}{ofr.Fg} = \frac{Carried\ Call\ Attempts'\ Flow\ Intensity}{Offered\ Call\ Attempts'\ Flow\ Intensity}.$$

This indicator is inspired from [2] indicator Answer Seizure Ratio (ASR).

6. INFORMATION SECURITY STAGE

Significant part of modern business-oriented communication systems applications is providing secured channels for message and data exchanging. As example there should be mentioned Security-as-a-Service (SecaaS) business model example that takes into account person authentication in communication systems, message integrity checking, and sensitive information leakage counteraction during message transmission via open (public) channels [7].

Practical application of mentioned features requires usage of subsidiary security infrastructures – digital certificates and public key distribution managements, encryption protocol management etc. Modelling of these services requires integration the specific information security stage into proposed communication system model (Fig.2).

The security service stage (Fig. 2) contains Entry and Service phases. In the Entry Phase, B-user is asked for his/her security needs. With probability Pz (zero service) B-user is not ready to pay (with time, efforts and money) for security service. With the complementary probability (1-Pz) special process and control units (virtual devices) take care for security. The process unit is used for extracting the security related headers (e.g. certificate and key management data) from inputted data flow.

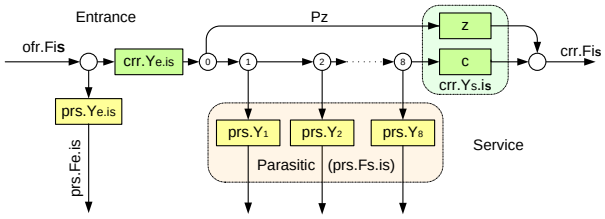

Fig. 3. Information Security (is) Service Stage with Entrance (e) and Service (s) Phases.

Establishing of secured communication channels requires cooperation of caller and called users with security infrastructure services, such as trusted third parties digital certificates management centers, public keys distributions servers etc. After successfully update and checking the security-related information by these services, communication between users can be started. In case of falling establishing the common security parameters, communications between users is cut off. The reasons for communication blocking are [8], [9], [10], [11]:

1. Failing of communication security protocol's parameters establishing;
2. Failing of message security attributes extraction;
3. Failing of message security attributes checking;
4. Invalid version of security protocol;
5. Invalid version of certificate;
6. Incorrect encryption/decryption keys;
7. Failing encryption/decryption procedure;
8. Incorrect digital signature;

Establishing the common security parameters by caller and called users can be recommence after fixed delay. In case of recurring communication blocking, value of delay is (exponentially) increased for preventing the infrastructure overloading and counteracting to deny-of-service attacks.

7. TELECOMMUNICATION SERVICE SYSTEM TRAFFIC CONCEPTS

In Fig. 4 the telecom network is presented as five service stages: A-terminal, Dialing, Switching, B-terminal Seizure and B-terminal. There are other stages in the system – included in A-User and B-User blocks, with their specifics.

The service stages of call attempts, in Fig 3are:

1. Demanding Stage: Calling (A)-users generate, in a Generate Device in the A-User block, intent call attempts [5], with intensity $int.Fa$. The intensity of suppressed intent call attempts is $sup.Fa$. Suppressed traffic is "The traffic that is withheld by users who anticipate a poor quality of service (QoS) performance" [5]. "At present, suitable algorithms for estimating suppressed traffic have not been defined" [15].

The intensity of demand call attempts [5] is $dem.Fa$. A performance indicator of A-User Demanding Stage is Adir (Demand –Intent Ratio):

$$Adir = \frac{dem.Fa}{int.Fa} = \frac{int.Fa - sup.Fa}{int.Fa}$$

Adir reflects demand, intent and suppressed call attempts and corresponds to the users' anticipations of a poor QoS performance.

2. Offering stage: This is a stage in which A-user adds call attempts to the demand ones. The additional call attempts are caused by repeated ($rep.Fa$) attempts. A-user decides whether to make the parasitic call attempts, (leaving the network), repeated or to terminate those (see terminator blocks in Fig. 4).

The intensity of all offered call attempts (demand, and repeated) trying to occupy A-terminals, in Fig.3, is $ofr.Fa$ A-terminals are considered as the first service stage servers, in the telecom network. From Fig. 4 follows: $ofr.Fa = dem.Fa + rep.Fa$

As a performance indicator of A-user Offering Stage, we propose Adem (Demand – Offered Ratio):

$$Adem = \frac{dem.Fa}{ofr.Fa} = \frac{dem.Fa}{dem.Fa + rep.Fa}$$

3. A-terminal Stage: In this stage A-terminals are occupied, effectively or not. The QoS indicator of A-terminal Stage (Qa) is:

$$Qa = \frac{crr.Fa}{ofr.Fa} \quad .$$

4. Dialing stage: The intensity of carried in A-terminals call attempts ($crr.Fa$) is equal to the intensity of the offered call attempts ($ofr.Fd$) to the Dialing Service Stage in the network – because the 'input' and 'output' are different roles of the same flow ($ofr.Fd = crr.Fa$). The QoS indicator of the Dialing Stage (Qd) is:

$$Qd = \frac{crr.Fd}{ofr.Fd}$$

5. Switching Stage: The QoS indicator of the Switching Stage (Qs) is:

$$Qs = \frac{crr.Fs}{ofr.Fs} \quad .$$

6. B-seizure Stage: The intend B-terminal may be busy or unavailable and this blocks call attempts. The QoS indicator of the B-Seizure Stage (Qz) is:

$$Qz = \frac{crr.Fz}{ofr.Fz} \quad .$$

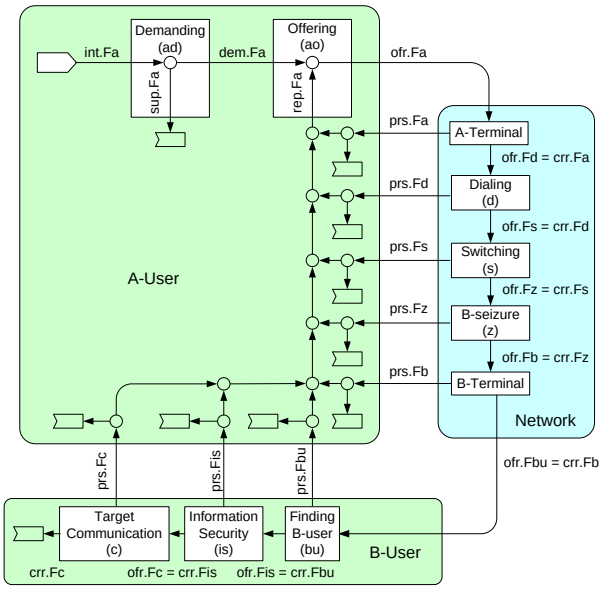

Fig.4 Schematic contributions to QoS in an overall telecom system, including users and Security Stage.

7. B-Terminal Stage: This stage corresponds to the B-terminal usage. The QoS indicator of the B-Terminal Stage (*Qb)* is:

$$Qb = \frac{crr.Fb}{ofr.Fb}$$

8. Finding B-user Stage: B-user may be absent, busy, tired etc. The QoS indicator of the Finding B-user Stage (*Qbu)* is:

$$Qbu = \frac{crr.Fbu}{ofr.Fbu}$$

9. Information Security Stage includes all necessary activities, ensuring security, if it is needed, as they are described in Section 4. The QoS indicator of the Information security Stage (*Qis)* is*:*

$$Qis = \frac{crr.Fis}{ofr.Fis} \quad .$$

10. Target Communication Stage. In this stage users exchange the target, of the call made, information. The QoS indicator of the Target Communication Stage (*Qc*) is:

$$Qc = \frac{crr.Fc}{ofr.Fc} \quad .$$

8. EFFICIENCY INDICATORS ON OVERALL NETWORK LEVEL

In our understanding, the Overall Network includes terminals and all network equipment. This means seven stages from A-Terminal to Information Security (Fig.4), inclusive. So, the QoS indicator of the Overall Network (Qnet) is:

$$Qnet = \frac{crr.Fis}{ofr.Fa}$$

Following Fig. 4 and equations in Section 7, it is checked directly that:

$$Qnet = \frac{crr.Fis}{ofr.Fa} = Qa\ Qd\ Qs\ Qz\ Qb\ Qbu\ Qis$$

9. EFFICIENCY INDICATOR ON OVERALL SYSTEM LEVEL

The Overall System Level includes users and all stages from intend call generation to fully successful completed communication. In terms of Fig.4, this means ten stages from Demanding to Target Communication, inclusive. Hence, the QoS indicator of the Overall Telecommunication System (*Qsys*) is:

$$Qsys = \frac{crr.Fc}{int.Fa}$$

Following Fig. 4 and equations in Section 7, it is checked directly that:

$$Qsys = \frac{crr.Fc}{int.Fa} = \frac{Adir}{Adem} Qa\ Qd\ Qs\ Qz\ Qb\ Qbu\ Qis\ Qc$$

The presented above indicators are flow-oriented. They are a base for time and traffic indicators construction, using the Theorem of Little and duration of service data. A step towards such indicators is made in [14].

10. NUMERICAL PREDICTION EXAMPLES OF THE OVERAL PERFORMANCE INDICATORS

We consider a model of Software Defined Network or virtual network (VNET) carrying Traffic Class 0. The VNET is with virtual channels switching, following the main method for traffic QoS guarantees – resource reservation.

The model is with: BPP (Bernoulli–Poisson–Pascal) input flow; repeated calls; limited number of homogeneous terminals; without suppressed call attempts; The calling (A) and called (B) terminals and users are considered separately, but in their interaction.

In Figures 5, 6 and 7, numerical results are presented using analytical and computer models, built following the methods explained in [14].

The numerical results are in the whole theoretical network load interval – overall terminal traffic of the A and B terminals equals of 0% to 100% of the number of all terminals in the network. The input parameters in the three figures are the same, excluding: (i) capacity of the network given as percentage of the number of all terminals in the system, causes blocking due to equipment insufficiency and (ii) the probability of repeated call attempts. The values of input parameters, in the presented numerical results, are typical for voice networks. Three cases have been considered:

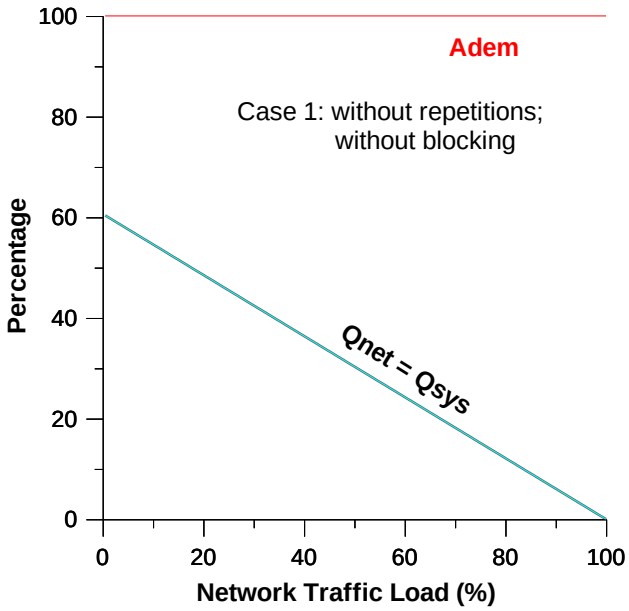

Fig. 5. Call Efficiency indicators Adem, *Qnet* and Qsys in Case 1. Adem = 1 and *Qnet* = Qsys, because there are not repeated attempts in the system. Adem is a constant 1. *Es* and *Ed* are decreasing monotonic functions.

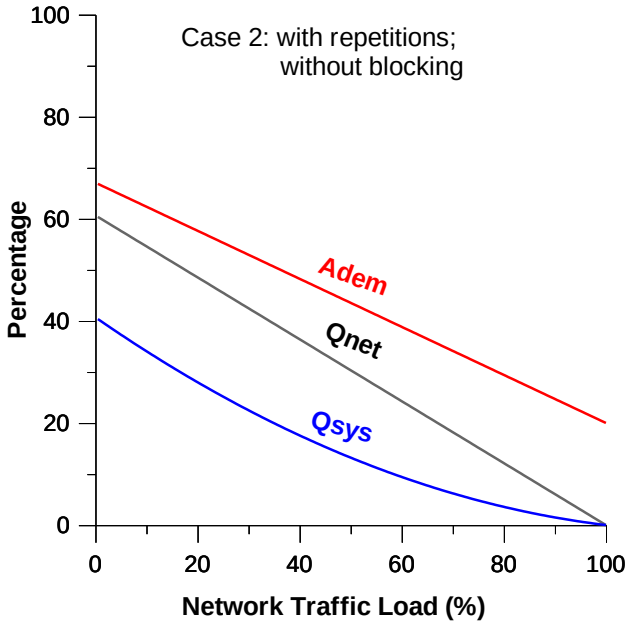

Fig. 6. Call Efficiency indicators Adem, Qnet and Qsys in Case 2. Repeated attempts make worse the performance considerably. Adem, Qnet and Qsys, are decreasing monotonic functions.

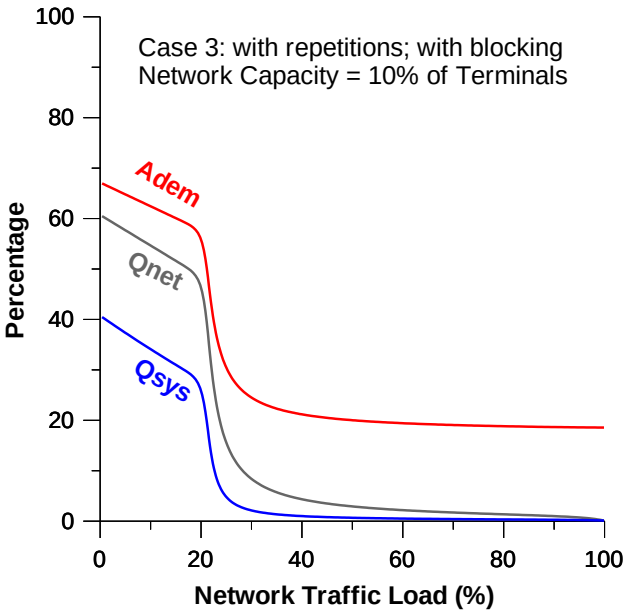

Fig.7s. Call Efficiency indicators Adem, Qnet and Qsys in Case 3. Blocking sharply make worse the system performance.

11. CONCLUSION

- The approach, explained, allows QoS presentation of every portion of the overall telecommunication system, consists composition of one or more consecutive stages. This may be used for stage performance comparison and more targeting QoS and QoE management.
- Introducing the security service stage give us opportunity to model not only public (open), but also secured communication channels between users. Taking into account the additional information flows, related to communication with trusted third parties, as well as increasing the traffic between users (adding the security related headers) allows increasing the precision of quality-of-service indicators estimations for real systems. The approach proposed is a step towards Security as a Service (SecaaS) practice.
- The QoS indicators considered are defined in terms of termination or continuation of call attempts' service, disregarding the reasons for this. An important task is modeling the QoS degradation factors as noise, distortions and others.

ACKNOWLEDGMENTS

This work is coordinated under EU COST Action IC 1304. The work was partially funded by Bulgarian NSF Projects DCOST 01/9 (work of S. Poryazov), and Bulgarian NSF Project DCOST 01/20 (work of E. Saranova).

REFERENCES

[1] M. Fiedler. Teletraffic models for Quality of Experience assessment. Tutorial at 23rd International Teletraffic Congress (ITC 23), San Francisco, CA, Sept. 2011. http://i-teletraffic.org/_Resources/Persistent/9269df1c3dca0bf58ee715c3b9afabbc71d4fb26/fiedler11.pdf (Accessed on 20.07.2017)

[2] ITU-T Rec. E.425 (03/2002). Internal automatic observations.

[3] ITU-T Recommendation E.800 (09/08), Definitions of terms related to quality of service.

[4] Stoyan Poryazov, Emiliya Saranova, Ivan Ganchev. Conceptual and Analytical Models for Quality of Overall Telecommunication Systems with QoS Guarantees Prediction. In: Ivan Ganchev, Rob van der Mai, J.L. (Hans) van den Berg (Editors). Autonomous Control for a Reliable Internet of Services: Methods, Models, Approaches, Techniques, Algorithms and Tools. Springer, LNCS, State-of-the-Art Surveys, 2018 (In print).

[5] ITU-T Recommendation E.600 (03/93), Terms and definitions of traffic engineering.

[6] S. A. Poryazov, E. T. Saranova. Some General Terminal and Network Teletraffic Equations in Virtual Circuit Switching Systems. Chapter 24 in: A.Nejat Ince, Ercan Topuz (Editors) Modeling and Simulation Tools for Emerging Telecommunications Networks. Springer Sciences+Business Media, LLC, USA 2006, pp. 471-505. ISBN-10: 0-387-32921-8 (HB).

[7] Furfaro, A.; Garro, A.; Tundis, A. (2014-10-01). "Towards Security as a Service (SecaaS): On the modeling of Security Services for Cloud Computing". 2014 International Carnahan Conference on Security Technology (ICCST): 1–6. doi:10.1109/CCST.2014.6986995

[8] RFC 2401. Security Architecture for the Internet Protocol. 1998/11

[9] RFC 4716. The Secure Shell (SSH) Public Key File Format. 2006/11

[10] RFC 5246. The Transport Layer Security (TLS) Protocol version 1.2. 2008/08;

[11] National Institute of Standards and Technology (December 2010). "Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program"

[12] RFC 4256. Generic Message Exchange Authentication for the Secure Shell Protocol (SSH). 2006/01

[13] RFC 5878. Transport Layer Security (TLS) Authorization Extensions. 2010/05

[14] Poryazov S., E. Saranova. Models of Telecommunication Networks with Virtual Channel Switching and Applications. Prof. Marin Drinov, Academic Publishing House, 2012, pp. 238. ISBN 978-954-322-540-8.

[15] [ITU-T Recommendation E.501] ITU-T Recommendation E.501: Estimation of Traffic Offered in The Network. (26th of May 1997).