ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
December 2012,
Vol. 5, No. (2):
Pgs. 199-204

The Impact of Client-Server Modalities on Cryptography

MOHAMMED MOSA AL-SHOMRANI[1],
MOHAMMAD. A.A. AL- RABABAH[2] and HUSSEIN AHMAD[3]

[1]King Abdulaziz University, Jeddah, KSA
[2]Northern Border University, KSA,
[3]Albalga Applied University Jordan

(Received: April 12, 2011; Accepted: June 04, 2011)

ABSTRACT

The performance of a mobile network is considered in the context of the given parameters QoS. We consider the known model QoS and problems of their use in mobile networks. In this paper proposed a mechanism to ensure QoS in mobile networks using Multiprotocol Label Switching (MPLS)

Key words:

INTRODUCTION

Modern computer networks are characterized by a sharp increase in traffic volume and the wide use of applications running in real-time multimedia applications, multicast applications. The performance of a modern computer networks is largely characterized by parameters such as quality of service (QoS). To ensure the QoS requirements have been developed: an integrated service (Integrated Services Architectures, IntServ)[1] and differentiated services (Differentiated Services, DifServ) [2, 3].

However, both of these architectures cannot be used in mobile networks, as mobile networks are essential parameters such as the fluctuation of the delay and packet loss. In this regard, mobile networks, it became necessary to improve the well-known and the development of new mechanisms to ensure the required level of QoS. In particular this applies to most typical representatives of the mobile networks - networks Ad Hoc, which is characterized by the absence of an express infrastructure [4].

The main reasons hindering the use of the architecture of IntServ networks Ad Hoc, are the following reasons:

- Module Access Control requires that each node has accurate information about the number of available resourses. However, obtaining such information in mobile ad hoc networks, hampered by a dynamic network structure.
- The movement of units and changes in the wireless transmission medium leads to frequent changes in data paths. Therefore, reservation made in one direction may become unusable and you want to backup on a new path that will increase the delay, overflow control network traffic.

- Reservation Protocol RSVP, used for the backup path in IntServ requires centralized management, which is absent in the network Ad Hoc.

The advantages of using relatively IntServ architecture DifServ include ease of implementation, efficiency, scalability, a small amount of proprietary information. In addition, low hardware complexity of the model DifServ the node, the lack of centralized control, the absence of an external signal and the resource reservation mechanism, allow us to consider the architecture DifServ, as the base for the provision of QoS in mobile networks, Ad Hoc. However, the architecture is focused on stationary DifServ computer network and does not take into account the dynamic nature of mobile networks and cannot directly be used in networks, Ad Hoc.

Analysis of existing solutions and publications. Currently, there are a number of schemes QoS for mobile networks, which represent the implementation of QoS at different levels of model OSI [5, 6] and can be represented by the following classes:

- Independent of the scheme;
- Implementation of QoS at the data link layer;
- Routing protocols based QoS.

Theoretical Consideration

Independent architecture is an implementation of QoS regardless of the level of the OSI model architectures like IntServ and DifServ. All traffic is classified into classes with different priority, depending on which provides the required quality of service.

Flexible QoS Model for mobile networks, the model FQMM [7], provides a unified implementation of the provision of quality services that are used in IntServ architectures and DifServ for different priority classes. Disadvantages associated with IntServ and DifServ inherent in the model FQMM. Architectures require a stable connection, the available bandwidth and information about the topology of the network, so FQMM works quite well in small mobile networks with low mobility nodes. It is also known for such independent schemes like SWAN [8], INSIGNIA [9].

Providing QoS in mobile networks is closely related to routing issues. In turn, taking into account the QoS routing requires not only find the shortest path from source to destination, but also to ensure that this route would have satisfied the terms of the qualities that constitute parameters required QoS. The analysis in the literature [10, 11] shows that the most effective for use in the Ad Hoc networks are reactive protocols that initiate the request for the formation of a route on demand. Currently, the Ad Hoc networks there are several routing algorithms CEDAR [12], TORA [13], AODV [14], DSR [15] that the formation of their way to a certain extent takes into account the parameters of QoS.

The most effective method of routing data in Ad Hoc networks, taking into account the desired QoS, the protocol suggests the use of Multiprotocol Label Switching (MultiProtocol Label Switching, MPLS) [16]. MPLS technology combines the capabilities of traffic management techniques inherent link-layer protocols, scalability and flexibility characteristic of the network layer. Network

The main advantages of MPLS over traditional routing are:

- Flexible support for QoS, integrated services and virtual private networks;
- Possibility to use to make routing decisions, not only the recipient's address, but other data;
- The separation of functionality between the kernel and the boundary area network, through which can be simplified structure of the core network routers, and increased their speed.
- MPLS implements mechanisms to assign a higher priority sensitive to network bandwidth traffic types, such as video streams.

Formulation of the problem. Further enhance MPLS related to the nature of network traffic. At present, almost all networks are multiservice, because information flows are formed by different agencies. Studies carried out in [17, 18,] confirmed that data flows and processes of their treatment processes are described with self-similar properties, which are taken into account when calculating the parameters of QoS.

Table 1: Distributions for the types of traffic

Type the traffic	Protocol	Distribution law	
		A	B
traffic data	TCP/IP	P, M	P, M, W
	AAL-3/4	M	M
Traffic transactions(interactive)	TCP/IP	P, M	P, M, W, LN
	AAL-3/4	M	M
Real-time traffic (video)	TCP/IP	P	P
	AAL-2	P	P
Real-time traffic (voice)	TCP/IP	P	P
	AAL-1	P	P

In most cases, capacity is planning and performance prediction using queuing theory. The law of distribution of traffic for different applications allows for calculation of parameters QoS, given the parameters of the distributions: expectation, variance and root mean square coefficient of variation. However, in practice, in many cases found that the results predicted by the analysis differ significantly from actual performance. On this basis, we can say that the solution to this problem belongs to the class of NP-complete problems. This problem is multifactor problem of dynamic programming. In[19] proposes an approach for solving problems related to QoS, and is a parameterized linear programming algorithm.

A distinctive feature of this work is the ability to process flows, taking into account the traffic characteristics. Analyze the types of traffic in multiservice networks, and associate with each type of traffic laws related distribution process, admission protocol units (A) and the distribution of the lengths of the protocol block ¬ Cove (B) (Table 1).

In Table. 1 the following notation:
M - the exponential;

W - Weibull (Weibull-Gnedenko);

P - Pareto;

LN - log-normal.

From Table 1 shows that in most cases, the nature of network traffic [20] obeys the Pareto distribution

The solution of the problem. Let us consider in more detail the use of the Pareto distribution to ensure the required QoS.

Let a graph of N vertices and L links, where each link l is defined weights vector consisting of m elements *wi (l)*, where $1 \le i \le m$. Considering only the weight of the additive relations, determined the most appropriate route of P from the transmitter to the receiver, taking into account QoS, satisfying the equation [19]:

$$w_i(P) = \sum_{l \in P} w_i(l) \le C_i \qquad \text{....(1)}$$

where *Ci* (for $1 \le i \le m$) - a restriction required by the user QoS. To obtain the "best" way, we can write the problem of finding the way, taking into account QoS in the form of an integer programming problem. For clarity of presentation, we restrict discussion of weighted connectionsm =2.

First, we introduce an integer vector flow *x c L* elements and the condition that xl = 1 if link l belongs to route *P, xl = 0* otherwise. In this case, the constraint (1) can be written in compact form [19]

$$wi(P) = cTx \le C1$$
$$w2(P) = dTx \le C2, \qquad (2)$$

where c and d - the first and second vector of weights of links of the graph, respectively. The problem with m = 2 links weights can be represented as [19]:

find *x* under the condition $Bx_l = b$, $x_l \in \{0,1\}$ for all *1≤ l ≤ L,*

where: *B* - matrix of dimension N × L links between the vertices of the graph,

b - vector of user requirements.

If *bi = 1, bj = -1*, and *bk = 0* for $k \neq i,j$, a solution of (2) is a possible path P from vertex *i* to vertex *j*. If there is another valid route, additional criteria may determine the "best" way. As you can see, the problem (2) with two or more connections weights *(m ≤ 2)* is NP-complete. Instead of (2), consider a multi-purpose integer programming problem without constraints(1):

$$\rightarrow min \qquad ...(3)$$

under the conditions: $Bx_l = b$, $x_l \in \{0,1\}$ for all *1 ≤ l ≤ L,*

Feasible solution x to (3) satisfies *Bxl = b* and *xl {0,1}* for all *1 ≤ l ≤ L*, and are optimal solutions, which are also minimize the objective function vector.

To find the Pareto optimal values are usually used secularization, to convert the vector into a real number, with the criterion of minimizing(3).

For m = 2 dimensions, the transformation is reduced to $R^2 \rightarrow R : \{c^T x, d^T x\} \rightarrow f\{c^T x, d^T x\}$, where *f* is subject to certain properties of monotonicity. The problem of scalar optimization[20]

$$f(c^T x, d^T x) \rightarrow \min \qquad ...(4)$$

under the conditions: for all *1 ≤ l ≤ L,*

returns the optimal solution *x * (f).* Explicit secularization function *f* is a linear function of the vector components , where λ1 and λ2 - positive real numbers.

Facilitation of problem (4) optimization of the network, if *xl {0,1}* for all *1 ≤ l ≤ L* is reduced to[19]:

$$\lambda_1 c^T x + \lambda_2 d^T x \rightarrow min \qquad ...(5)$$

under the conditions : $Bx_l = b$, $x_l \in \{0,1\}$ for all *1 ≤ l ≤ L,*

Varying λ ≥ 0, we find a Pareto optimal values for the original problem (3). However, even when varying λ in all the possible non-negative integers, not all Pareto optimal values from (3) will be guaranteed to be found. For any m> 1, the objective function is λTw, where λ - m-dimensional vector, as well as the vector w. If λTw = a, where a - a constant, and it shows that the vector λ is orthogonal with respect to the vector w. Graph the piecewise linear curve shown in Figure 1. If λ1 = 0 (or $\lambda \rightarrow \infty$), we obtain the shortest path in a graph with a single connection weight, taken from the second component of the balance relations w.

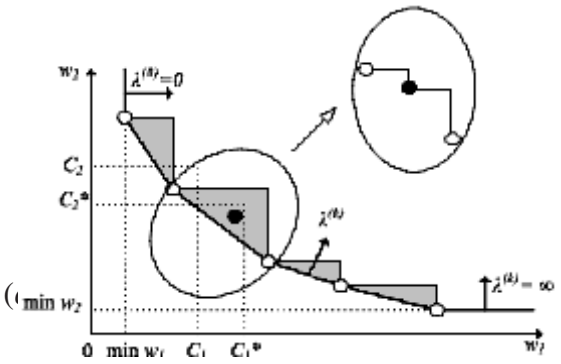

Fig. 1: The piecewise linear curve, to find the optimal value of the Pareto

Hence, in Figure 1, a line parallel to the axis w1, is the weight of the shortest path, and a line parallel to the axis corresponds to only a weight w2 shortest path first component of the balance relations w (ë = 0). These values (the smallest w1, the smallest w2) are the absolute minimum for the (w1, w2), and they can be easily obtained, for example, using the algorithm finding the shortest path Daystar

Permissible region lies above the curve (thick line) for the condition (5). If at least one vertex is surrounded by the constraints C1 and C2, then this will be the only solution under the given constraints QoS. If the constraints C1 * and C2 * do not surround the point of extremism, the remainder of the triangular area to scan for possible integer solutions (that way). If there is only one internal extremism point between two consecutive extremely points on the curve of a compromise, ellipsoidal

insert shows the exact curve of the resulting compromise between these extreme points.

Fig. 2 shows that there are two types of boundary curves. First - connects the extreme point $\lambda = 0$ and $\lambda \to \infty$. The intersection of horizontal and vertical lines drawn through these points are extreme coordinates (min w1, min w2), and the like are the only optimal point. The second case is the connection point extreme $\lambda = 0$ and $\lambda \to \infty$, all extreme points on this line are Pareto-optimal if the value of w1 extreme points reduce the value of w2 must increase. It is clear that all the other curves are problems between these extremes. Continuous sequential function w2 passes through the point $\lambda = 0$ and $\lambda \to \infty$. The tangent at any point reduces the search area in the plane of the feasible solutions of (w1, w2) of all points on a tangent.

Improving the efficiency of MPLS. Further enhance MPLS related to the nature of network traffic is possible by taking into account the traffic characteristics, in particular its self-similarity.

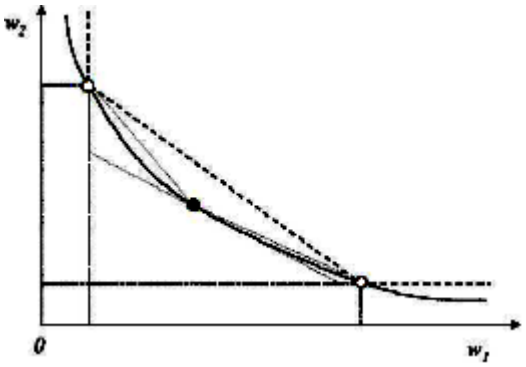

Fig. 2: Schedule of determining the search area in the plane of the feasible solutions of (w1,w2)

This method allows to optimize the procedure for the separation of incoming packets for transmission on one of the ways to appropriate LSP, depending on the step chart (Figure 1), which shows the optimal values of flow vectors Pareto. This, in turn, can increase the level of QoS.

When high-intensity loading of each packet received from the ways (and the corresponding physical channels) will be uniform. The main advantage of this method is its simplicity, and as a consequence, the possibility of implementing an algorithm based on it with a small time complexity. Routing algorithm that takes into account the requirements of different traffic flows and takes into account the resources available at various transit stations and on different nodes, called the routing algorithm based on constraints. In essence, the network, which uses an algorithm, always knows about the level of the current network usage, current capacity and parameters of the adopted QoS.

CONCLUSIONS

Analysis of the literature shows that the most effective technology for the implementation of QoS in mobile networks is MPLS.

Further increase in the efficiency of mobile networks with MPLS technology is associated with taking into account peculiarities of mobile networks and network traffic. Substantiates the effectiveness of the Pareto distribution for the analysis of traffic in mobile networks.

Proposed and developed criteria for dividing flows in the most optimal routes in terms of given parameters QoS.

REFERENCES

1. Blake S, Black D, Carlson M, etc, An architecture for differentiated services, IETF RFC 2475, (1998).
2. Nichols K, Jacobson V, and Zhang L, A two-bit differentiated services architecture for the internet, RFC 2638, (1999).
3. Chakrabarti S. and Mishra A, QoS issues in Ad Hoc Wireless, IEEE Communications Magazine, (2001).
4. Demetrios Z, A Glance at Quality of Services in Mobile Ad-Hoc Networks, Seminar in Mobile Ad Hoc Networks, (2001).
5. Xiao H., Seahand W K G, Lo A. and Chua K. C, A flexible quality of service model for

mobile ad-hoc networks, IEEE VTC2000-spring, Japon/Tokyo, (2000).

6. Ahn G, Campbell A, Veres A., and Sun L –H, Supporting service differentiation for real-time and best-effort traffic in stateless wireless ad hoc networks (swan) IEEE Transactions on Mobile Computing, **1**(3): 192-207 (2002).
7. Lee SB, Ahn GS, and Campbell A Improving udp and tcp performance in mobile ad hoc networks with insignia, IEEE Communications Magazine, **39(**6): (2001).
8. Adjih C, Clausen T Jacquet P etc., Optimized link state routing protocol, Internet-Draft Version 08, IETF, (2003).
9. Das S R Perkins C E and Royer E Performance comparison of two on-demand routing protocols for ad hoc networks, Proceedings of the IEEE Conference on Computer Communications, pages 3–12, (2000).
10. Sivakumar R Sinha P and Bharghavan V Cedar: A core-extraction distributed ad hoc routing algorithm, *IEEE Journal on Selected Areas in Communications,* **17**(8): 1454-1465 (1999).
11. Park V. and Corson S, Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Speci¯cation, Internet Draft, (2001).
12. Das S Perkins C. E. and Royer E. M., Ad hoc on demand distance vector (AODV) routing, Internet-Draft Version 13, IETF, (2003).
13. Broch J Johnson D B. and Maltz D A The dynamic source routing protocol for mobile ad hoc networks, Internet Draft Version 08 IETF (2003).
14. Yeh C H Mouftah H. T, and Hassanein H., Signaling and QoS Guarantees in Mobile Ad Hoc Networks, IEEE, (2002).
15. Riedi R Willinger W, Toward an Improved Understanding of Network Traffic Dynamics, Self-Similar Network Traffic and Performance Evaluation, (2000).
16. Feldman A Whitt W Fitting Mixtures of Exponentials to Long-Tail Distributions to Analyze Network Performance Models, (1998).