TELECOMMUNICATIONS AND INFORMATICS SYSTEMS' ROLE IN SECURITY ASSURANCE FOR EMERGENCY SITUATIONS. USAGE OF THE ALL-IP NETWORKS, NGI NETWORKS OR INTERNET AS MEDIUM FOR ALERTS TRANSMISSION

Nicolae-Dorel CONSTANTINESCU[1]

Acest articol introduce problema alertării în situaţii de urgenţă folosind ca suport de comunicaţie Internetul, o clasifică drept una de interoperabilitate a sistemelor informatice de securitate şi încearcă a îi formula o soluţie pe baza instrumentelor IT deja consacrate, cum este utilizarea de standarde deschise. Se propune astfel completarea unor serii de standarde bazate pe XML ca de exemplu CAP, EDXL, TSO, cu elemente de suport al calităţii serviciului folosind convenţii de prioritizare, în vederea unei ulterioare unificări şi implementări ca standard pentru aplicaţiile utilizate în situaţii de urgenţă şi producătorii de echipamente de reţea.

This article introduces possibility of using Internet as communication support during the emergency situations alerting process, classifying it as one of security information systems interoperability and trying to offer a solution based on already established IT tools, like the use of open standards. It therefore proposes to supplement a series of XML-based standards like CAP, EDXL, TSO, with elements supporting the quality of service, using prioritization conventions, in view of further unification and implementation as a standard for emergency applications and network infrastructure equipment manufacturers.

Keywords: emergency, alerting, CAP, EDXL, TSO, DSCP

1. Introduction

Security studies often refer to a category named *asymmetry*, which means the inequitable disproportion of a forces opposition. The term semantics can also be identified within the *emergency situations* definition, when the impact of some negatives events cannot be managed by using the standard resources. Telecommunications and information technology have the capability and must be used in order to represent an ally in the battle generated by the emergencies.

Interoperability represents one of the main problems and therefore every study related to the security systems tries to provide us with a solution.

[1] PhD student, Automatic Control and Computers Faculty, University POLITEHNICA of Bucharest, e-mail: dorel_nic@yahoo.com

As communication means, ALL-IP networks, NGI (Next Generation Internet) type networks or the current Internet benefit of certain features that make them attractive and bring challenges for using them in emergencies. One of these challenges consists in providing the required level of Quality of Service delivered over the Internet. Nowadays, much attention is paid to *quality* as a domain. ISO 9000 standard defines quality as the degree by which native characteristics (of an entity as product or service) meet the demands and expectations (of its users). Providing Internet services to customers involves a contract between the provider and the client, a so-called SLA (Service Level Agreement), regarding the conditions of service delivery or the values (metrics) agreed on specific parameters that the service must comply with. When applying to IT Services, SLAs are often built using the ITIL (Information Technology Infrastructure Library) specifications, a set of IT concepts and best practices (service support, service delivery, management of infrastructure etc.). An item of SLA is SLO (Service Level Objectives) which includes the measurable characteristics of SLAs, such as availability, response time, recovery time etc., also called QoS (Quality of Service) parameters. Network policies terminology is detailed in RFC 3198 [1].

The current process of migration from old generation networks including PSTN, radio and TV broadcast networks or the old Internet (which is not capable of transporting packets in real time), where different services depended on dedicated infrastructure, to NGN networks, has many implications, including on emergency communications. This expected transition to NGN will bring many benefits, as the availability of a wide range of innovative new services, greater control and an easy way of choosing or changing the range of contracted services. At the same time, migration to NGN raises some problems. Aside from economic concerns (irregular distribution depending on regional development, very low - not economically feasible - price of voice calls, etc.), technologically speaking, communication through these systems must provide the appropriate level of security, according to type of traffic, information security principles and legislative rules. Speaking about the emergency communications issue, it is mandatory for these networks to preserve certain features, such as the possibility of making a call to 112 emergency services in conjunction with providing the caller location. [2]

A type of service that could be introduced within the current Internet and should be supported by NGN, is the emergency alerts reception. In this paper, we discuss certain issues related to the quality of the service (QoS) on the subject of emergency alerts transmission over IP networks and we propose a mechanism of prioritization, having in mind the idea of special tagging of the packets from the emergency message structure (this can be applied to both population alerting messages and to the messages traveling between the various sensors and

processing units, connected through Internet). Perhaps a few seconds of delay or some delay variation (jitter) are not very important, when delivering emergency messages to people, but in case of congestion, delay or packet loss can greatly increase; for emergency communication between devices (like the command to shutdown a critical installation in a refinery, before an earthquake), the above elements are always important. From a security management perspective, one can see that the problem to be solved is one of interoperability, understood in the context of Alberts C2 theory [3]. Information should be created and structured in an interoperable format and then sent to the destination (all using IT tools). The problem of emergency communications it's intensively studied, both from political and technical point of view. This paper is different in the fact that it joins both side's principles and adopts a practical solution, showing a way interoperability can be achieved.

2. IP convergence of communication architectures. QoS in Internet

The current trend of migration of voice, data, video, all with mobility (*triple play on the move*), to IP, increasingly more visible, and the convergence of the three core areas of competence (networks, services and applications) [4] ensures us that the problem of providing emergency services, using such infrastructure as support, is actual and worth investigating. Native Internet is a *best effort* service, using the simplest model of QoS, where management of queues in routers is usually done in FIFO (first in first out) order and controlling just *where* to send packages. For the implementation of QoS requirements in Internet, the IETF (Internet Engineering Task Force) proposed two main approaches: Integrated Services – IntServ [5] and Differentiated Services – DiffServ [6].

IntServ uses a QoS assurance model by signaling, in which hosts signal their QoS requirements to network, using a reservation protocol, Resource Reservation Protocol (RSVP). QoS signaling and reservation is performed individually, for each unidirectional flow between two applications, uniquely identified by the group: source IP address, source port number, destination IP address, destination port number and transport protocol. IntServ proposes two new classes of service in addition to best effort, namely the Guaranteed Service [7], for real time applications requiring fixed delay limits, and Controlled Load Service [8], for applications that require only an enhanced best effort service, i.e. a behavior similar to best effort, in low loaded networks, and control and allocation mechanisms, in high load conditions. IntServ is implemented through four components: the signaling protocol (RSVP), the admission control routine, the classifier and the packet scheduler. To declare its resource requirements, an application must specify the desired QoS parameters in a list called *flowspec*.

Flowspec is carried by the reservation protocol, sent to the admission control to test whether it is acceptable (if for the new flow can be guaranteed the required QoS without affecting the previous allocations), and finally used to parameterize the packet scheduling algorithm (using queues and mechanisms such as timers). The classifier is mapping out each new came package in a class, where each packet receives the same treatment from the scheduler. The disadvantage of IntServ approach is scalability. Amount of state information increases proportionally with the number of flows. This massively supplements storage and processing requirements for backbone routers. IntServ requires identification and treatment of each flow, packets planning and queues management for each flow as well. The control system complexity and cost increases with the number of flows, because there is no unique label to identify a flow or a group of flows with similar performance requirements (Service Level Specifications) and traffic characteristics. Moreover, RSVP signaling does not have a release message, so a refresh message is periodically necessary to confirm the resource request; a connection closes only if a refresh message is not received within a certain period. So, even if the IP flow has been completed, the resource is not released immediately and signaling messages are still consuming bandwidth. Guaranteed service must be implemented in a generalized way. Controlled-load service can be implemented incrementally, by focusing its functionalities and the ones of the reservation protocol on the congested nodes of a domain and tunneling RSVP messages in other parts of the domain. Requirements on routers are firm, all of them must support RSVP, admission control, packet classification and scheduling. In fact, this mandatory requirement for routers to be able to reserve resources, in order to provide QoS for specific user packet flows, which further required to store the status of flows in the routers, proved to be impractical, so until IntServ was completely standardized, a new standard have arisen, namely DiffServ. While IntServ uses the method of QoS assurance for each flow, DiffServ divides traffic into classes, for which a certain type of service (CoS - Class of Service) will be provided, using the principle of the *aggregate quality of service*. To achieve traffic classification, packets must be marked, accordingly to assigned class. IPv4 packet header contains Type of Service (TOS) byte, with the following interpretation:

Table 1

Interpretation of ToS field from IPv4 packet's header

	0-2	3	4	5	6	7
RFC791	Precedence	Delay	Throughput	Reliability	Reserved=0	Reserved=0
RFC2474, RFC2475, RFC3168	DSCP				ECN	

Within the classification called IP Precedence, the first three bits of TOS byte are used, resulting in eight classes of precedence. Next three bits (Delay, Throughput and Reliability) are used to specify a value of compromise between these three performance parameters. Bits 6, 7 are reserved for future use. Full interpretation can be found in RFC 791 [9].

DiffServ architecture redefines the meaning of IPv4 Type of Service byte (Traffic Class in IPv6 [10].). The first six bits of this byte (now having the name DS - Differentiated Services) are called DSCP (Differentiated Services Code Point) and used to differentiate the treatment a packet receives at every network node. The other two bits are called ECN (Explicit Congestion Notification) and are used independently of DiffServ, to mark the network congestion, without dropping packets and therefore avoiding retransmissions [11]. Once DiffServ identifies a packet at a node as belonging to a particular class, it applies to it an appropriate procedure for transmission, based on its DSCP code (range of delay, delay variation limits, etc.). This procedure is called PHB (Per Hop Behavior). Packet classification, tagging, followed by specific treatment at each network node, creates prerequisites for a scalable QoS architecture, suitable for all applications.

3. Emergency alerting using the Internet

The Internet has already proven to be a communication channel with great potential in crises. During the attacks of September 11, fixed telephone communications have ceased to operate, due to overload. In this situation, millions of people used the Internet to communicate [12]. Some even used the Internet to make phone calls, bypassing the conventional telephone infrastructure [13]. Social networks, "Safe and Well" list, the Ipoki application are examples of the potential of Internet use for emergencies [14].

4. The structure of communication and alerting messages in emergencies

XML had become the *lingua franca* used by software applications for data exchange. In support of the effective communication in emergencies, for the creation of so-called Common Operational Picture or for emergency alerting, and in response to interoperability requirements, languages such as EDXL (Emergency Data Exchange Language), TSO (Tactical Situation Object) or CAP (Common Alerting Protocol) have been created; all of them are intended to facilitate the requirements described above. EDXL is joint effort, intended to define a family of specifications for data exchange, compatible with the National Incident Management System (NIMS) in US, comprising notification of incidents, reports on the statements, reports on states, request and dispatching of resources,

analytical data, geospatial information, identification and authentication [15]. Tactical Situation Object (TSO) is a proposed standard for the exchange of information during disasters and emergency management. A TSO can describe a diverse range of events, resources and tasks involved in ongoing operations [16]. Common Alerting Protocol (CAP) [17] offers an open digital message format, for all types of alerts and notifications. It is not referring to any particular application or method of telecommunication. All these message formats are built using XML. Therefore, they are intended to be digitally stored and transmitted via computer networks. Elements of emergency messages are XML structured, so all these types of messages share a common format, which makes implementation of new functionalities, in each of them, a straightforward task.

5. Proposal to supplement the message structure

Before such messages are placed on the access link of some router in the network, one issue must be considered. It is that of speed and accuracy by which this network, not always dedicated only to emergency traffic, will carry the message to the destination. Depending on the emergency degree, which is usually very high in this case, emergency messages, practically the packets that form them, should be given high priority over other types of traffic flowing through that shared infrastructure. For example, within a past research program, OASIS - FP6 (Open Advanced Systems for Disaster Management - Framework Programme 6), some simulations were performed at the Romanian and Moldovian common border, on a potential flood disaster. The method of structuring and sharing the Common Operational Picture was the TSO message, which, as shown in figure, was sent on a 100km section, over the Internet, entering inevitably into competition with other types of traffic.

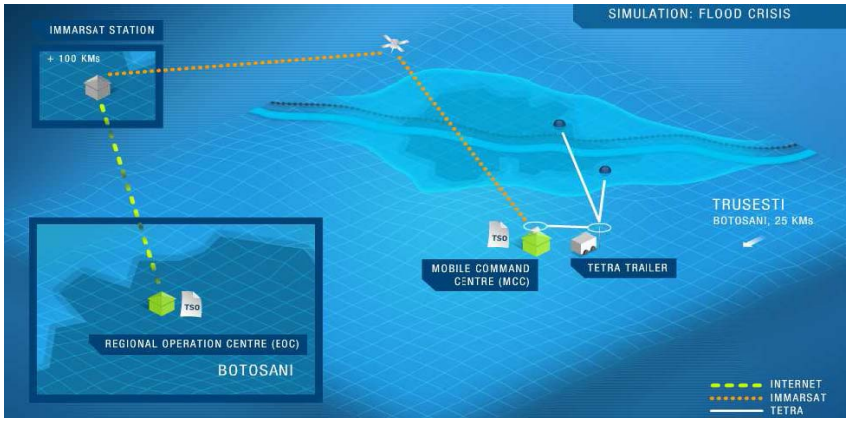

Fig. 1 – the route of an emergency message through various networks, includind Internet [19]

Therefore, one aspect that the standards mentioned above do not analyze, but which must be paid careful attention to when using public networks like the Internet, as transport medium, is the Quality of Service. Internet, as we previously suggested, represents an interesting environment to benefit from in emergency situations.

In the next section, we propose an approach consistent with DiffServ, a solution that operate both at Application layer and IP layer, by adding a new component to the emergency messages sent over the Internet and by tagging the packets from their structure, to specify the nature of messages and quality of service.The DOM structure of emergency messages may be supplemented with the TRANSMISSION_SPEC element, which is necessary for the specification of a set of parameters that will have meaning and will be interpreted by emergency applications. A mark will be applied on all packets of emergency message structure, which will be evaluated by the software of routers that a packet founds on its way to the destination.

The software system for generating emergency messages will have, in addition to the function of creating XML messages containing useful information for public agencies, the function of setting the TRANSMISSION_ SPEC item and writing into the header of IP packets the corresponding DSCP field. The software of routers will implement into DiffServ behavior the reservation of certain predefined DSCP assignations, in IP Critical (101) class of precedence. Emergency messages can therefore be classified as information, notification, warning and alert, as bellow:

Table 2

Proposal of classification for emergency messages

Message type	**DSCP code**
Information	101001
Notification	101011
Warning	101101
Alert	101111

The above table presents a proposal for classification of emergency traffic, which is backwards compatible with IP Precedence.

Table 3

The elements of TRANSMISSION_SPEC

TRANSMISSION_SPEC	The element from the XML structure of emergency messages which state the transport parameters and QoS assignation
SOURCE_ADDRESS	Public IP address of the machine on which messages are sent
SOURCE_PORT	Source port
DESTINATION_ADDRESS	Public IP address of the machine on which messages are received
DESTINATION_PORT	Destination port
DSCP_CODE	DSCP coding according to message type

Four combinations are left available for other high priority network traffic (IP telephony, streaming, etc.). IP addresses and ports are used to uniquely identify the machines and services from which the alerting application is running. On the reverse path, source and destination change places and a client application will know where to send the confirmation of receipt. Alert server will have the capability to mark IP packets with DSCP code properly. This task can be achieved at application level or for the entire communications system. TRANSMISSION_ SPEC will be generated by application, complying with transmission requirements and message type selection, done by the emergency application user.

5. 1 DOM of TRANSMISSION_ SPEC

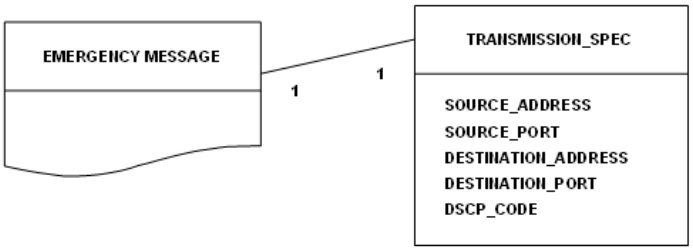

Fig. 2 – DOM TRANSMISSION_SPEC

5. 2 Usage proposal

Below is the proposal for the usage of TRANSMISSION_SPEC element, in context of a CAP message:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "urn:oasis:names:tc:emergency:cap:1.1">
...
<transmission_spec>
<source_address>89.120.45.15</source_address>
<source_port>4001<source_port>
<destination_address>212.36.189.72<destination_address>
<destination_port>5200<destination_port>
<dscp_code>101101</dscp_code>
</transmission_spec>
...
</alert>
```

In the next figure it can be observed the Differentiated Services Code Point in default state, unmarked (packet captured with Wireshark [20]):

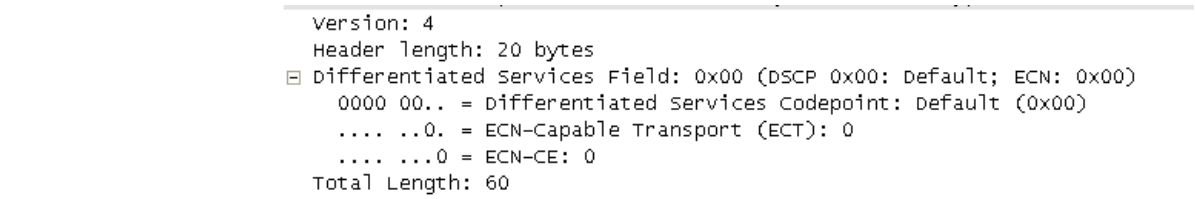

Fig. 3 – header of a best effort packet

In the following figure we can observe the packet is marked with code 101101, corresponding to a *Warning* message type, complying with the classification advanced in Table 2.

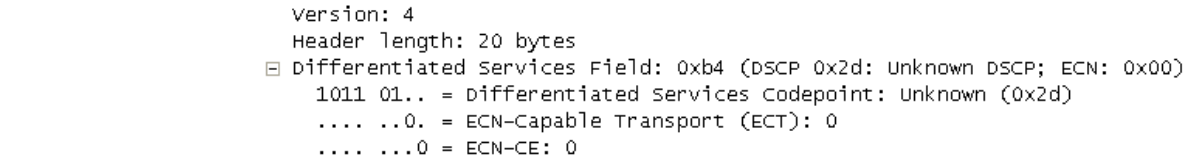

Fig. 4 – header of a *Warning* packet

6. Conclusion

The QoS issue within IP networks usually arises in view of applications such as audio-video broadcast, teleconferencing and videoconferencing or IP telephony (VoIP). These are examples of services sensitive to QoS parameters, both in normal, but especially in emergency situations, when competition over resources suddenly increases and the most common problem is congestion.

IP applications and services, particular to emergencies, represent an important category along with the services listed above (those which are used both in usual situations and in emergency situations), and should be also, or especially, provided with QoS. Further, warning messages in emergency situations represent only part of the IP traffic that is generated in such situations. In this paper, we propose a qualitative solution, on intermediary *edge-to-edge* sections (DiffServ domains) to solve QoS problem of warning messages. A pure DiffServ approach has the advantage of scalability, but does not offer *end-to-end* QoS guarantees. A quantitative solution, that does offer the *end-to-end* guarantees, involves resource reservation, as stated by the terms of IntServ, but has the well-known disadvantages as well.

The idea of traffic parameters inclusion within emergency messages formats and tagging of packets from their structure, can only work by having standards bodies and manufacturers support. In IPv6, two fields of the IP packet header can be used to mark traffic: Traffic Class field, of eight bits, which could lead to an equivalent operating process as using the IPv4 TOS field, or Flow

Label field, of twenty bits, which would open a wide range of possibilities for classification.

R E F E R E N C E S

[1] *** RFC 3198, http://tools.ietf.org/html/rfc3198
[2] *Nicolae-Dorel Constantinescu*, Finding the caller location information for calls to the emergency services (Localizarea apelantului la serviciul pentru apel de urgență), Revista Română de Automatică şi Informatică, nr. 1 2009
[3] *D. Alberts et all*, Understanding the Information Age Warfare, http://www.dodccrp.org/files/Alberts_UIAW.pdf, accesat 2 iunie 2010
[4] *** Building the Carrier-Class IP Next-Generation Network, http://www.cisco.com/en/US/prod/collateral/routers/ps5763/prod_white_paper0900aecd802e2a52_ns573_Networking_Solutions_White_Paper.html, accesat mai 2010
[5] *** RFC 1633, http://www.ietf.org/rfc/rfc1633.txt
[6] *** RFC 2475, http://tools.ietf.org/html/rfc2475
[7] *** RFC 2212, http://www.ietf.org/rfc/rfc2212.txt
[8] *** RFC 2211, http://tools.ietf.org/html/rfc2211
[9] *** RFC 791, http://www.ietf.org/rfc/rfc791.txt
[10] *** RFC 2474, RFC 2475, http://tools.ietf.org/html/rfc2474, http://tools.ietf.org/html/rfc2475
[11] *** RFC 3168, http://tools.ietf.org/html/rfc3168
[12] *Theresa L. Jefferson*, Using the internet to communicate during a crisis, The journal of information and knowledge management systems, Vol. 36 No. 2, 2006, pp. 139-142, Emerald Group Publishing Limited
[13] *** *W. Knight*, Internet aids US disaster communications, http://www.newscientist.com/article/dn1293-internet-aids-us-disaster-communications.html, accesat 2 iunie 2010
[14] *Nicolae-Dorel Constantinescu*, New prospects of exploiting Geographical Information Systems for Emergency Alerting (Noi perspective de exploatare a Sistemelor Informatice Geografice pentru avertizarea în Situațiile de Urgență), Conferința Strategii XXI, UNAP, aprile 2010
[15] *** http://xml.coverpages.org/edxl.html
[16] *** http://www.tacticalsituationobject.org
[17] *** http://www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected_DOM.pdf, descărcat 2 iunie 2010
[18] http://www.tacticalsituationobject.org/docs/CWA_15931-1.pdf
[19] *** http://www.oasis-fp6.org/documents/Final%20Event%20General%20Presentation%20V2.pdf, descărcat 2 iunie 2010
[20] *** http://www.wireshark.org/