E711 - A Public Emergency Wireless Phone System

Victor Matos and Ben Blake
Cleveland State University
2121 Euclid Ave.
Cleveland, OH 44115
v.matos@csuohio.edu; benblake@csuohio.edu

ABSTRACT
This paper introduces the conceptual design of a new information technology integrating wireless telephony and Internet services to assist in locating lost or displaced people in a moment of crisis. This public safety service is based on a novel text messaging mobile-phone emergency service called "E711" which informs that the caller is safe and well. The proposed E711 messages are delivered as *guaranteed* SMS packets to a centralized web emergency registry operated by a public safety organization. Finding the whereabouts of a victim could be done by consulting the entries of this registry. The public could access the emergency database in a variety of ways including Internet searches and phone calls. Optionally, *non-guarantee* E711 SMS messages are forwarded to family and friends. We provide an algorithm to automatically recognize critical flow changes of E711 packets and dynamically adapt congested network gateways for optimum delivery. We argue that in case of high network traffic, the E711 system has a better chance of success than voice services such as E911 or person-to-person communication.

Keywords: Technology for public safety, Wireless communication network, Emergency SMS phone service, Congestion management.

1. INTRODUCTION

Calamities occurring on the early years of the 21st century are collectively responsible for hundred of thousands of casualties, billions of dollars in losses, and millions of displaced and homeless victims. Most studies of these disasters expose extremely poor to unacceptable levels of response to the situations [1, 2, 3, 4, 13, 14]. A notorious inadequacy highlighted by those tragedies is the lack of rapid, simple, and efficient methods to facilitate communication between friends and family members concerned about victims of the tragedy. Telecommunications and web technologies could and should provide a great deal of support in coordinating relief, warning potential victims of imminent dangers, reuniting people, and quickly informing the rest of the world about the reality of a catastrophic event [10, 13]. The worldwide success of wireless communications suggests a new set of possibilities for societal interaction not contemplated a few years ago. Mobile telecommunication units are becoming more available in all regions of the planet. In an early paper [12] we argue that it is reasonable to believe that soon most people – regardless of their economic status and location in the world - will have the ability to enjoy the benefits brought by wireless information technology and web engineering advancements. Consequently, many new technologies and services devised to leverage this new state of global connectedness will emerge [11].

This paper describes a worldwide public safety service that uses wireless phones and text-messages. The proposed system centrally collects and organizes emergency messages and disseminates the information to both disaster relief effort teams and to friends and family of the victim. This new public service - called E711 or "*I am OK*"- is intended as a first step in the task of informing family and friends about the well-being of an affected individual. The E711 messages will be carried as small text messages (SMS) [6]. Cellular text-messaging offers an effective, fast and inexpensive mechanism for mass communication. These SMS merits have been recognized and adopted in various public and private networks for implementing emergency strategies. For instance, regional authorities use it to alert people located in a given territory of an imminent weather threat, an industrial disaster, or even a terrorist attack. Local organizations broadcast to their affiliate members important safety messages ranging from potential catastrophic disasters to cancellation of classes. The main characteristic of these strategies is the top-down hierarchical structure of information dissemination. Under this model the *authorities* inform the *public* about the potential threat. Messages are sent from an informed entity (local government, company, University) to a large, local audience.

Our E711 model differs from those approaches in its *peer-to-peer* nature in which victims inform other people about their current situation after an event has already developed. Existing SMS broadcast systems transmit information to the victims while the proposed E711 gathers information about them. We believe that both emergency strategies: broadcasting and E711 could easily co-exist and complement each other. One obvious problem with both emergency technologies is that they will not operate in areas where wireless phone service is unavailable or SMS is not operational. In addition, certain political circumstances may prohibit SMS messaging. Fortunately, broadcasting and E711 services are currently viable in most of the world's densely populated areas. Furthermore, delivery of E711 messages for roaming users and those who connect to the phone network using other technologies such as satellite services, will be treated in the same transparent manner as users who attempts to deliver emergency E711 messages in their local service area.

Our work uses an abstraction of network gateways as the centerpiece of the system. The gateways are subjected to a policy-driven strategy that continuously recognizes variations on the patterns of SMS traffic and allows them to self-adjust whenever it becomes necessary. This strategy results in a highly optimized network behavior that provides support for *lossless* E711 flow. Our mathematical model extends the work of [7, 8] by introducing and emphasizing the role of emergency SMS packets on self-adapting policy driven networks.

The remainder of this paper is as follows: the next section provides background to understand the characteristics of a typical wireless phone network and identify the text messaging bottleneck. The third section describes in detail the E711 emergency system and

introduces a methodology for handling sporadic network congestion and adjusting the gateways to optimally operate under pressure conditions. The last section presents conclusion and suggestions for future research.

2. BACKGROUND

2.1 Text Messages

The SMS standard is used by cell phones to transmit small pieces of textual data (typically 140 characters per package). There are enhanced versions of the SMS service – such as EMS and MMS - which allow multi-media objects to be included in the package [6, 7, 9, 13]. These types of long, more complex messages are not included in this discussion. In an individual geographic region, cell phone carriers receive a restricted set of frequencies. Typically, a governing body allots frequencies to carriers per geographic region. Each carrier subdivides these frequencies into two distinct sets. The larger of these two sets (about 90% of the spectrum) is commonly referred to as the *voice channels* and the smaller one is called the *control channels*.

The voice channels carry voice data in the form of wireless phone conversations. In a simplistic model, two channels or frequencies are required for a single phone conversation. One of those frequencies is used for sending data and another frequency for receiving. The control channels - often referred to as "out-of-band" frequencies - assist the mobile unit in locating the strongest signal, provide synchronization information, communicate call set-up information, and accomplish other signal-level tasks. When a call request is either sent or answered, the control channels communicate information to the mobile unit as to which frequencies/channels will be allotted for the voice data of that particular call.

In an effective phone network enough bandwidth must be set aside in the control channels to service busy periods. This out-of-band pre-allocation strategy creates unused bandwidth during non-busy periods. Phone network operators use SMS messages to fill idle time and more completely utilize the bandwidth of the control channels. To further promote SMS service, most telecommunication operators allow users to make connections between their networks and the Internet. By enhancing the way in which users can exchange text messages with one another, the operators not only provide a convenient service but also create new lines of revenues. However, the opening of the wireless phone network to the Internet brings its own set of vulnerability issues [5], observe that an excessive amount of SMS traffic can overwhelm the capacity of the control bandwidth that has been set aside for sporadic data.

Network gateways (SMSG) provide an ideal instrument for network automation and self-control. A SMSG represents a programmable device that interconnects a wireless network to the data network [15]. Each gateway handles all connections to SMSCs, retransmission in the case of temporary connection failures, and generation of statistics and billing reports. A SMSG manages message traffic, congestion, and routing between SMSCs and applications. Additionally, SMSGs often support multiple protocols in order to communicate with a variety of networks [6].

2.2 Network Topology and E711 Architecture

The main goals of the "*I am OK*" service are to reliably collect, safely store and promptly forward wellness information about persons within a geographic region during the impact or post-impact phases of a disaster. Figure 1 illustrates a typical scenario with a victim sending an E711 text message to tell family that he is fine. The emergency registry stores the message and if possible, forwards a copy of it to the victim's friends and family. The current message is *chronologically* stored in the registry from which it could be accessed at a later time using the Internet or a phone.

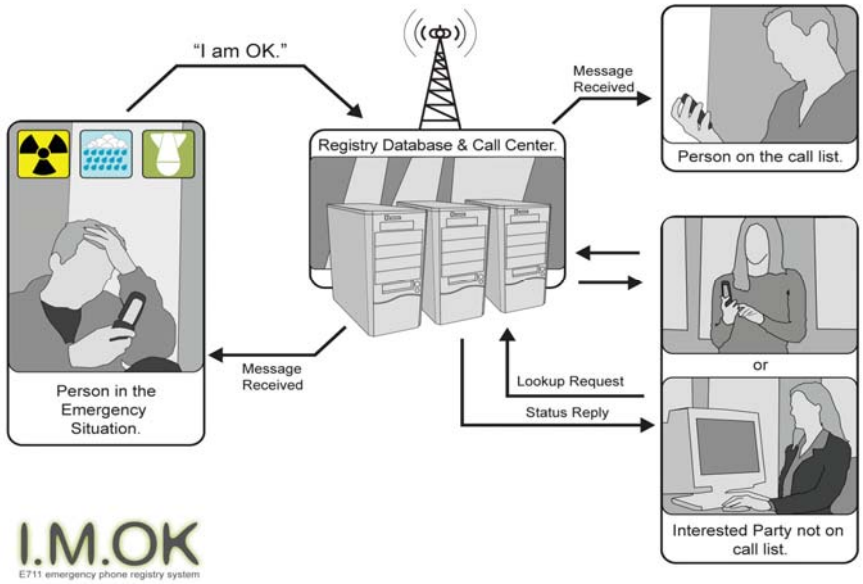

Figure 1. The E711 Emergency Phone Registry System

A more detailed view of the E711 signal exchange process is shown in Figure 2. The E711 service consists of two phases: *notification* (victim-to-family) and *consultation* (family-to-registry). The notification phase is subdivided into two steps *original posting* and *message spawning*. Posting occurs when the high priority E711 signal originates from an active mobile handset. The message is sent through the system to the emergency registry database (ERD) . After entering the data in the centralized ERD, the emergency center sends a reception *acknowledgement* (ack) back to the mobile unit. The *ack* signal is treated as a priority message to reassure the sender of delivery and avoid unnecessary transmission. Copies of the original message are spawned and sent to every phone number and internet address on the notification list of the original E711 sender. The spawned copies belong in the E711 non-urgent message category. Demoting those important types of signals to a non-critical denomination is intended as a safeguard mechanism to prevent competition with the more relevant messages sent by the victims.

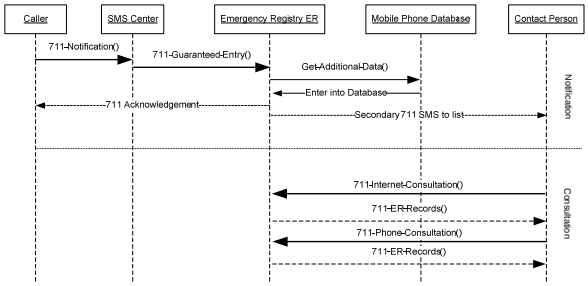

Figure 2. Phases of the E711 Service: Notification and Consultation.

The lower portion of Fig. 2 depicts an ERD query. E711 consultation is performed by friends and family who either failed to receive copies of the "I am OK" messages or are not on someone's emergency list. These concerned friends and family may connect to the E711 registry to ascertain the condition of individuals. A search into the database provides a historical sequence of the messages posted by a victim. Tracing those records allows concerned persons to find out the state of a love one, particularly if no direct voice communication has been made with the victim. Several strategies could be used to implement the consultation process, for example using a handheld device for sending and receiving an E711 query text message, browsing the Internet, or making a voice phone call to a human or automated answering system.

2.3 Composition and Classes of E711 messages

Instead of asking the E711 user to tediously tap keys on the phone to compose their lines of text, the emergency messages are largely assembled by an internal mobile phone application. There are four types of E711 messages; (a) *those sent from a distressed individual* to inform about his/her situation, (b) *acknowledgement messages* sent by the network to the victim to acknowledge accepting the emergency message, (c) *messages spawned by a distress message* to reach family and friends, and (d*) inquiry messages* made asynchronously as requests for the state of a victim. Due to the reduced size limitations (140 chars under GSM standard), E711 messages must encode in a compact way as much data as possible. Figure 3 suggests the layout of a typical E711 distress message containing the sender's phone number, GPS coordinates, timestamp, and optional message.

SMS Control Header	SMS Data
Sender Phone No. Phone ID Carrier etc.	Message Type (E711) Family-Friends Contact number(s) Latitude & Longitude Timestamp Optional Text Message

Figure 3. Layout of Fields in a Typical E711 Message

The default text for an E711 packet is the expression "*I am OK*", however the internal phone application could provide a list of other predefined or customized messages. It is also clear that a free format option should be available to enter any short text the victim may want to supply. The E711 system could be extended to provide other services, for instance messages could be used by rescue crews to locate lost people, by health care providers to assist a person requesting emergency medical attention when that person can not speak or the phone lines are busy, or in medical applications transferring vital signs of a monitored patient to a medical provider, and so on.

3. MANAGING NETWORK CONGESTION

3.1 Identifying Operational Goals

Several solutions have been proposed for handling congested networks carrying SMS packets [7, 8, 15]. In those solutions the phone gateways recognize the high flow of text messages and self regulate their intake, out-take, and local retention factors. By modifying those parameters the operator hopes to provide a solution to the instantaneous changes of load and topology experienced by the network. We extend the policy driven congestion management work of [7, 8] by providing a gateway level solution to a congested network that carries three classes of messages: (1) *Priority* (important material such as person-to-person text communication), (2) *Non-priority* communications (such as commercial advertisement, bulk non-critical messaging), and (3) *Emergency E711* packets. We also recognize the need to dynamically declare (and rescind) "*State of Emergency"* on nodes seen very high E711 circulation. Placing a node into a state of emergency involves the transitory acquisition of voice channels to offload the SMS traffic.

To implement a harmonious and efficient environment in which the E711 system could co-exist with other type of non-critical text messages, we expect the network gateways to be responsible for the enforcement of the following six performance policies

1. Priority and E711 messages will be delivered in no more than δ_{max} seconds.
2. At most a β_{max} percentage of non-priority messages will be delayed by the gateway and eventually delivered in more than δ_{max} seconds.
3. The gateways must route the highest possible number of messages.
4. A 100% of E711 messages will be accepted by the gateways.
5. A 100% of accepted E711 messages will be routed to the central emergency database.
6. If the proportion of E711 messages arriving to a gateway exceeds, the limit placed on the control variable σ_{711} the gateway will enter into a *State of Emergency* and notify authorities of a potential crisis.

These rules provide a framework for the behavioral description of service characterizing the agreement made between provider and customers. The first three performance policies are common for policy-driven networks carrying priority and non-priority messages [7, 8]. The last three are new to the model and address the particular needs of E711 emergency messages.

3.2 Modeling the Gateway's Performance Criteria

A simplified view of a typical gateway is depicted in Figure 4. It emphasizes the presence of input and output ports, internal control elements, a traffic matrix that keeps track of how each input channel diverts its load on the outgoing lines, disk storage and operational parameters whose settings determine the node's behavior. The equations in Table 1 provide a mechanism to optimize operations of such a gateway subject to the six listed constraints in section 3.1. The objective function (Eq. 1a) pursues the maximization of SMS flow while keeping the delivery promises in agreement with the physical limitations of the network devices. The equations (1) to (5) from Table 1 are similar to those in [7, 8]. However equation (6) is new; it provides a computationally correct approach for estimating the percentage of non-priority message that must be delayed in the gateway's disk storage in order to operate inside the promised performance margins. In the following discussion E711 messages will be considered the top-tier of priority messages.

SMS packets arrive to the input ports at different rates; α_i represents the rate (msg/sec) of those incoming packets allowed by the *i*-th port. The matrix T_{ij} keeps track of the portion of messages which came to each input port-*i* and was sent to each output port-*j* in the last τ seconds. The SMSG *Traffic Estimator* is responsible for monitoring the actual traffic and maintaining accurate values for α_i and the traffic matrix T_{ij}.

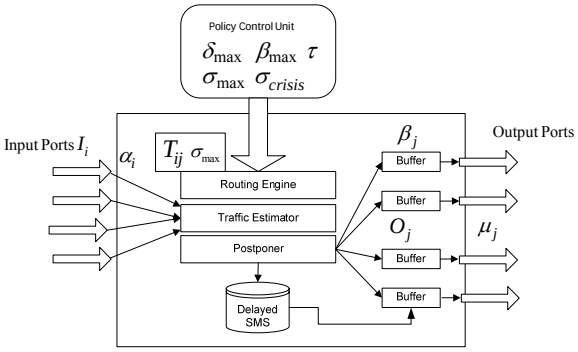

Figure 4. Layout of a Typical Gateway Showing its Policy-Driven Control Elements.

The portion ($1-(\sigma_{max} + \sigma_{711})$) appearing in equations (1b) and (6) represents the percentage on non-priority messages accepted by the gateway. Each output port *j* has a small fast buffer on which messages are queued before been dispatched to their corresponding destination; μ_j indicates the rate of service of output port *j* (msg/sec.). The expression β_j is the current fraction of non-priority packets destined to outgoing port *j* that can not be accommodated in its fast buffer and must be delayed. None of the β_j values could exceed β_{max} that has been promised by the service provider as an operational limit to deferred data (Eq. 3b). The delay decision is made by the *Routing Engine*; deferred packets are placed in local disk storage.

Equation (1a) expresses the need to exploit the combined number of outgoing messages forwarded by the gateway. The term O_j represents the total output emerging from the *j*-th output port. Equation (2a) states that the rate of service of port *j* (μ_j) is limited and can not be exceeded by the total traffic sent to that port. The messages waiting for service at the *j*-th port are the result of combining all type of input messages arriving on the different *i* ports ($\sum_i \alpha_i T_{ij}$).

TABLE 1. Optimization Model for Network Gateway Carrying E711 SMS Messages.

$$Maximize \sum_j O_j \qquad \text{(Eq. 1a)}$$

$$O_j = \sum_i \alpha_i T_{ij} (1 - (1 - (\sigma_{\max} + \sigma_{711}))\beta_j) \qquad \text{(Eq. 1b)}$$

Subject to the boundary conditions

$$D_j \le \mu_j \quad \forall j \qquad \text{(Eq. 2a)}$$

where

$$D_j = \sum_i \alpha_i T_{ij} (1 - (1 - (\sigma_{\max} + \sigma_{711}))\beta_{\max}) \qquad \text{(Eq. 2b)}$$

and

$$\alpha_{\max} \ge I_i \ge \alpha_i \ge 0 \quad \forall i \qquad \text{(Eq. 3a)}$$

$$\beta_{\max} \ge \beta_j \ge 0 \quad \forall j \qquad \text{(Eq. 3b)}$$

$$O_j \le \sum_i \alpha_i T_{ij} \quad \forall j \qquad \text{(Eq. 4)}$$

$$O_j \le \mu_j \quad \forall j \qquad \text{(Eq. 5)}$$

$$\beta_j = \max\left[0, \frac{(1 - (\sigma_{\max} + \sigma_{711})) * (D_j - \mu_j)}{\sum_i \alpha_i T_{ij}}\right] \forall j$$

(Eq. 6)

Notation:

α_{max}	Maximum rate of input traffic
α_i	Acceptance rate of input port *i*
β_{max}	Maximum rate of delayed non-priority messages
β_j	Percentage of non-priority messages delayed at port j
I_i	Input traffic at port i
O_j	Output traffic emerging from port j
$(\sigma_{max} + \sigma_{711})$	Maximum percentage of priority and E711 messages combined
T_{ij}	Traffic matrix
μ_j	Service capacity of port j
τ	Length of policy re-evaluation interval

The expression $(1-(1-(\sigma_{max} + \sigma_{711}))\ \beta_{max})$ is the fraction of messages (including priority, emergency and non-priority) to be forwarded. Out of this fraction the operator is allowed to delay up to β_{max} messages from each port in order to ensure its promise of "good" service. Equation (4) indicates that messages intended for an output port could exceed the actual number of packets O_j forwarded by the port. If that event occurs the excess packets are held in the SMSG disk storage. In extreme cases some non-priority packets are discarded. Equation (5) indicates that output ports dispatching capacity is limited and cannot be overridden by current load.

Equation (6) is an indicator of the percentage of non-priority messages that must be held on disk to maintain the service agreement between the network operator and its customers. The value of β_j is 0 for non-congested ports. On congested output ports, β_j represents the proportion of non-priority messages the SMSG *Postponer* will route to disk instead of the *j*-th fast buffer.

3.3 Finding an Optimum Solution for the E711 SMSG Performance Model

Regulating the flow of incoming packets and the postponement of non-priority outgoing packets is essential for the ideal operation of the SMS gateways. The linear programming system of equations in Table 1 is periodically computed to adjust the values of α_i and β_j. Those parameters respectively indicate (a) the rate at which input ports should accept messages when the local gateway is congested but there is not a major emergency, and (b) the amount of non-priority messages that should be placed by the *Postponer* into the *Delayed SMS* disk to keep the system in an optimal state.

The extreme emergency values achieved by α_i and β_j are zero and one. An α_i equal to zero commands the i-th port to accept only emergency messages and reject all other classes of SMS packets, whereas and (α_i =1) suggests that all input messages are taken. Similarly, a postponement β_j value reaching a minimum of zero typifies and ideal delivery condition in which outgoing messages destined to the j-th gate are placed on the port's fast queue for immediate transmission. On the contrary, a value (β_j =1) suggests the highest port congestion and mandates that all deferrable messages be temporarily held in disk for future transmission. In case of extreme congestion E711 messages are saved on the local disk with the highest priority for future forwarding and in this situation non-priority packets could be purged from disk to make room for E711 messages.

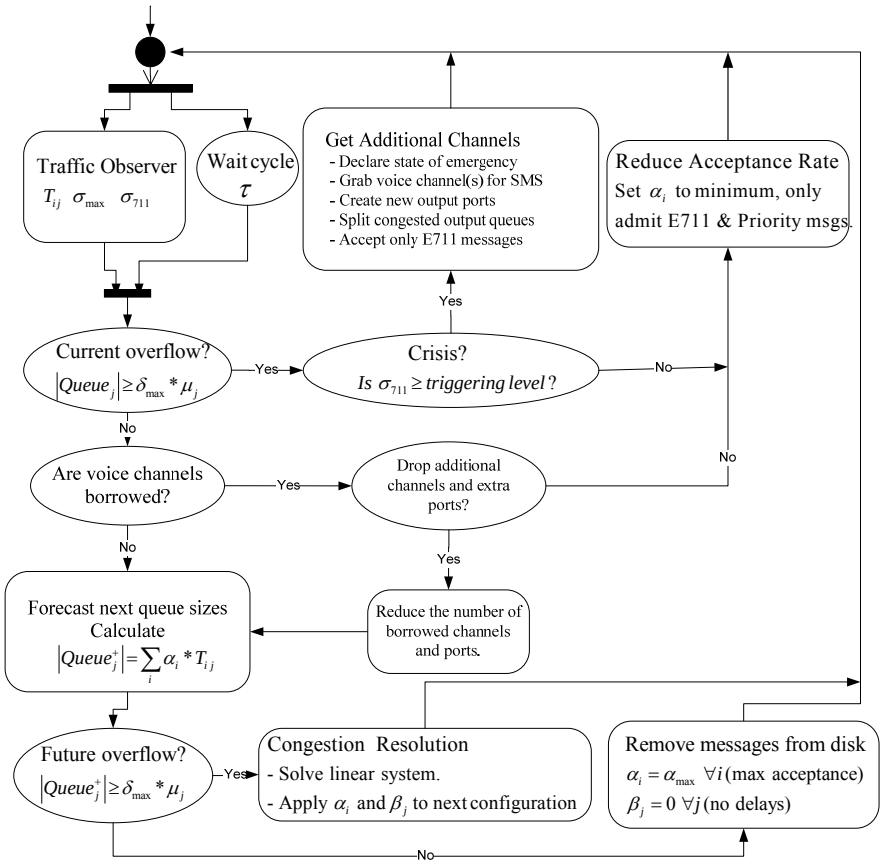

Figure 5: Policy-Based SMS Congestion and Crisis Management Algorithm

3.4 Gateway Congestion/Emergency Management Algorithm

The algorithm implementing the gateway's policy-based SMS congestion and crisis management strategy is depicted in Figure 5. The main control logic contains a number of steps inside of a closed loop that is repeated every τ seconds. A cycle begins with the activation of the *Traffic Observer* unit which is

responsible for continuously monitoring traffic and tallying the number and kind of different messages moving through the gateway.

The following scenario is presented to illustrate the optimization algorithm for a gateway located in a zone where a natural disaster occurs. The example assumes an initial gateway configuration of three input ports, three output ports, and priority messages promised to be delivered in no more than 20 seconds ($\delta_{max} \leq 20$).

The traffic matrix remains fixed and uniform throughout the example with messages from each input port spread evenly over the original three output ports. Initially we assume the flow of messages through the ports is heavy, but at equilibrium. Each input port accepts 50 messages per second and each output port delivers 50 messages per second. The system remains in this state from time 0 to time 40 with the *Traffic Observer* operating every 10 seconds. During these first 40 seconds the algorithm of Figure 5 loops around the outermost path with all messages delivered in a timely manner.

At time 40 an external event triggers a large increase in the number of incoming messages. Instead of 50 messages per second each input port now receives 100 messages per second. The next scheduled operation of the *Traffic Observer* at time 50 discovers 500 messages queued at each output port. Assume this configuration is well below the emergency-level threshold for σ_{711} to take any action and the algorithm remains in a *non-crisis* state. The same traffic flow continues for the next ten second interval after which the *Traffic Observer* finds 1000 messages queued on each output port at time 60. At this point let us assume the messages in each queue is $\left|Queue_j\right| - 1 = \delta_{\max} * \mu_j$, which is just below the threshold to trigger overflow.

Assume the increased flow on the input ports continues for the next ten seconds and at time 70 the *Traffic Observer* discovers 1500 messages in each of the three output queues. At this point the algorithm reacts to the excess of incoming messages because the queues are above their threshold levels. Let us also assume that a surge of E711 messages have arrived and they are sufficient to trigger a *crisis* situation. Since there is an excess of messages on each output port, the algorithm temporarily creates three new output ports, duplicating the capacity of the original output ports. The new temporary ports borrow bandwidth from voice channels (for simplicity, assume the additional bandwidth is of the same size of the current control channel). All the accepted messages waiting to be forwarded are given to the corresponding new output ports. This decision clears the original queues to resume forwarding messages. Furthermore, input ports are instructed to only allow into the gateway new E711 messages.

For this illustration we will consider the new input rate on each port decreases to 30 messages per second and the six output ports each deliver 50 messages per second.

From time 70-to-80 the 900 newly arriving messages are easily sent through the original output ports and 500 queued messages are sent from each newly created temporary output port. The system remains in this state until time 100 when the queues of the temporary ports cleared out. At this point the algorithm deletes the temporary output ports, relinquishes the borrowed voice channels, and reverts the gateway to the non-crisis state.

If the actual rate of E711 flowing through the gateway had not been sufficient enough to trigger a crisis, the SMSG could deal with congestion in a more relax way [7, 8]. First it is imperative to predict whether or not a queue will overflow in the next τ cycle. This foretelling could by done by asking the algorithm to use the present traffic patterns and sum the current contribution of each of the input ports at their current rate of arrival ($\sum_i \alpha_i * T_{ij}$). If no overrunning of a port is anticipated, the system is instructed to operate ideally by accepting all messages and delaying nothing ($\alpha_i=\alpha_{max}$, $\beta_j=0$). If the flow-control algorithm discovers a future queue overflow condition, the linear programming system shown in Table 1 is solved to discover the optimum next gateway configuration. In this way an appropriate solution balancing the rate of acceptance for input messages (α_i s) and postponement of non-priority output messages (β_j s) will help in keeping the promises made by the network provider.

4. CONCLUSION

This article introduces the wireless phone E711 ("I am OK") protocol and a conceptual model for its efficient implementation. The primary goal of E711 is to inform that the caller is safe and well. We believe the E711 service will prove to be effective in a crisis, it could (and should) be adopted by any number of countries.

The E711 system requires a software application embedded in the user's mobile unit and a modified type of policy-based management software on the SMS gateways. The phone application assembles a text message including identification of the caller, a timestamp, and location data. E711 messages are delivered as guaranteed SMS packets to a singular emergency registry operated by a public safety organization. Entries on this registry could be accessed by the public in a variety of ways. Optionally, a number of non-guarantee SMS messages can be forwarded to family and friends. In cases of extreme congestion, the E711 service dynamically reconfigures the delivery policy of the affected gateways and temporarily borrows voice channels guaranteeing the delivery of emergency text messages.

Future work includes solving problems such as (a) deciding the location and management of the emergency database (ERD). This issue offers an interesting opportunity for global humanitarian cooperation. Several equally appealing options appear such as a unique database for the entire world, or perhaps one run by individual country/region(s), etc. (b) finding efficient algorithms for acquiring additional bandwidth to cope with congestion when in crisis mode along with distributing messages among the existing and temporary ports created in response to burst of emergency messages, (c) simulation of the enhanced gateways looking at a variety of traffic patterns.

Adopting the proposed E711 service would facilitate relief efforts by providing useful survivor data. We believe these brief "I am OK" messages would have a significant emotional impact in comforting separated friends and family members affected by catastrophes.

REFERENCES

[1] American Civil Liberties Union. *USA Patriot Act* (11/14/2003). Available at http:// www.aclu.org/safefree/resources/17343res20031114.html Accessed October 2006.

[2] Congress of the United States of America. *Uniting And Strengthening America By Providing Appropriate Tools Required Intercepting And Obstructing Terrorism* (*USA Patriot Act) Act Of 2001. Public Law 107–56.* OCT. 26, 2001.

[3] Department of Homeland Security. *The National Plan for Research and Development In Support of Critical Infrastructure Protection* – 2004. Available at www.dhs.gov. Accessed October 2006.

[4] Department of Homeland Security. *Threats and Protection Advisory System.* Available at http://www.dhs.gov. Accessed October 2006.

[5] Enck W., Traynor P., McDaniel P., La Porta T. Exploiting Open Functionality in SMS-Capable Cellular Networks. *CCS2005 - 12th ACM Conference on Computer and Communications Security*, Alexandria, Virginia,USA. November 2005

[6] Global System for Mobile Communications. Web site at www.gsmworld.com. Accessed October 2006.

[7] Gonzalez-Prieto, A. et al. Policy-Based Congestion Management for an SMS Gateway. *Proceedings of the Fifth IEEE International Workshop on Polices for Distributed Systems and Networks*, 2004.

[8] Gonzalez-Prieto, A., Stadler, R.. Evaluating a Congestion Management Architecture for SMS Gateways. *9th IFIP/IEEE International Symposium on Integrated Network Management* Nice, France, 2005.

[9] Gwenaël Le Bodic, Vodafone. *Mobile Messaging SMS, EMS and MMS*, 2nd Edition (Wiley & Sons, 2005).

[10] Lowestein, M. Preparing for the 'Next Katrina' . *Wireless Week - Online Edition.* Nov. 1, 2005. Available at: www.wirelessweek.com. Accessed October 2006.

[11] Martin, C. Dianne and Elaine Yale Weltz (1998). From Awareness to Action: Integrating Ethics and Social Responsibility across the Computer Science Curriculum. *Third Report from the Project ImpactCS Steering Committee*. Available at http://www.seas.gwu.edu/~impactcs/paper3/ toc.html. Accessed October 2006.

[12] Matos, Victor and Blake, Ben. 'I am OK' - A Conceptual Model for a Global Emergency System and Its Societal Impact*. International Journal of Technology, Knowledge and Society. Vol. 2 No. 5,* pp.7-18, January 2007.

[13] Patterson, David. Rescuing Our Families, Our Neighbors, and Ourselves. *Communications of the ACM*, *48(11)*, 2005.

[14] U.S. House of Representatives. *A Failure of Initiative - Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*. Available at ww.gpoacess.gov/congress/index.html. Accessed February 15, 2006.

[15] Verna, D., Simplifying Network Administration Using Policy-Based Management, *IEEE Network, 16(2),* 2002. 20-26.

Received: Oct. 2008. Accepted: Jan. 2009