Challenges of Optimizing Common Alerting Protocol for SMS based GSM Devices in Last-Mile Hazard Warnings in Sri Lanka

First Nuwan Waidyanatha, Second D. Dias, and Third H. Purasinghe

Abstract - **The aim of the Last-Mile Hazard Warning System (LM-HWS) is to deploy various alert and notification wireless technologies intended to reduce the vulnerability of local communities to natural and manmade hazards in Sri Lanka.[1] The project adopts an "all-hazards, all-media" approach designed around a set of five wireless communication technologies. The pilot project entitled, "Evaluating Last-Mile Hazard Information Dissemination", or the "HazInfo Project", involved deployment, training, and field-testing of the technologies, in various combinations, across 32 tsunami-affected villages, using the "Common Alerting Protocol[2]" (CAP) for data interchange with content provided in three languages (English, Sinhalese and Tamil). Results to date suggest that the basic internetworking arrangement at lower technical layers has proven to be reasonably robust and reliable but that a key challenge remains in the upper layers of application software and content provision. This is evident in the apparent difficulties faced when implementing CAP messaging over a LM-HWS that included two GSM Technology solutions. Lessons learned from silent tests and live exercises point to several key bottlenecks in the GSM solutions where the integrity of CAP messages is compromised due to problems associated with technological boundaries, technical difficulties, software interoperability, and direct human intervention. Those working with content standards and development of software for hazard information systems must consider closely the interoperability issues at various layers of interconnectivity as well as compromising technological uncertainty caused by human mishaps. As field trials suggest, text based alerting such as cell broadcasting (or short message services) can not be introduced for public alerting until a common content standard is agreed upon that takes into consideration the restrictions imposed as a result of miniaturization of mobile handheld devices that prevent from displaying unambiguous alert messages. This paper reports on findings from a series of field tests conducted in Sri Lanka to compare the reliability of the two GSM solutions with their relative effectiveness in terms of alert and notification capabilities in the last-mile of an early warning system**

Index Terms - All-Hazard, Cell Broadcast Short Message Service, Common Alerting Protocol, Global Standard Mobile Last-Mile, Warning

I. INTRODUCTION

In December 2005, LIRNEAsia, an ICT policy and reform research organization, initiated a research project to evaluate the "last-of-the-mile" communication component of an all-hazards warning system for Sri Lanka. The project entitled, "Evaluating Last-Mile Hazard Information Dissemination", or the "HazInfo Project", work was carried out with the aid of a grant from the International Development Research Centre (IDRC), Ottawa Canada. Its research design was based on recommendations of a "participatory concept paper" for a national early warning system (NEWS:SL) completed in the months following the 2004 tsunami [10].

Fig. 1 illustrates the subsystems of an end-to-end early warning system. The paper noted that although the issuing of public hazard warnings was the responsibility of the

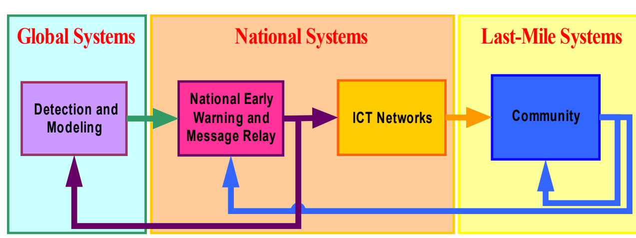


Fig. 1 end-to-end chain of system for early warning

[1] Research Project: Evaluating Last-Mile Hazard Information Dissemination (HazInfo). 2006. Available http://www.lirneasia.net/projects/current-projects/evaluatinglast-mile-hazard-information-dissemination-hazinfo/

[2] Botterell, Art and Addams-Moring, Ronja. (2007). Public warning in the networked age: open standards to the rescue. Communications *of the ACM*, 30 (7), 59-60.

government, it is unlikely that the Last-Mile of such a system can be provided solely by government. Rather, it requires a partnership of all concerned including government, private and non-government sectors.

This paper discusses 2 of the 5 ICTs used in the research project, namely the Nokia 6600 Mobile Handset with the Microimage developed Multilanguage J2ME alerting applet and the Dialog-University-of-Moratuwa developed Remote Alarm Device (RAD) with a GSM-Module/Microcontroller. The Alerts were delivered to the last-mile via these two GSM Devices and Wireless Mobile Handheld Phones. In the case of the Nokia 6600 the messages were delivered in all 3 National Languages: Sinahala, Tamil, and English; where as the RAD would receive English text messages followed by voice instructions in Sinhala, Tamil, and English over an FM receiver. The authors are thankful of the partial sponsorship provided by the HazInfo technology partners: Dialog Telekom Ltd. for this work.

The research proposal of this project defined six specific research parameters for assessment: reliability of different wireless devices for transmitting messages, effectiveness of devices for alert and notification, impact of the technology on community organizational structure, effectiveness of the training regime, gender specific concerns, and integration of the wireless technology into the daily activities of the villages. This paper will focus on the first two parameters concerning the reliability and effectiveness of wireless technologies for providing hazard warnings to villages participating in the LM-HWS project.

LM-HWS assessed the wireless technologies, selected for their diverse communication paths and different features. The technologies were deployed in communities in a heterogeneous configuration. The research team also acknowledged the importance of incorporating "bi-directional" capabilities at the village level so that devices could provide communities with means to inquire of situations and inform local hazards to the Sarvodaya HIH (upstream communication).

II. LM-HWS ARCHITECTURE

The HazInfo project involves a non-government organization (NGO) Sarvodaya[3] and is established on a governance structure whereby this organization provides project oversight, training, and operates a Hazard

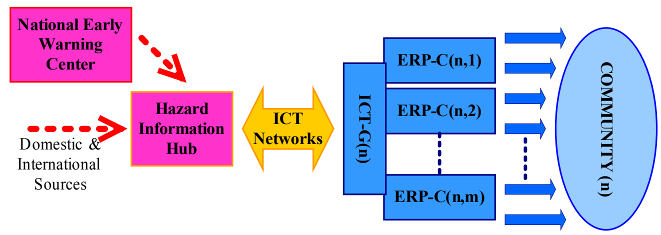


Fig. 2 - end-to-end hazard information communication architecture of the LM-HWS; where messages received at the HIH are relayed to the villages.

Information Hub (HIH) for the monitoring of hazard threats and dissemination of warning messages to local communities within the Sarvodaya network of villages. Each of the 32 participating communities varies in size from 150 – 1000 households.

The LM-HWS architecture depicted in Fig. 2 complements the traditional public alerting system design usually established by local and/or national governments. A traditional public alerting system issues warnings directly to communities via broadcast media such as television and radio, or through designated public address (PA) systems. By contrast, the LM-HWS project architecture establishes a closed user group of first responders, who are equipped with addressable wireless devices for receiving bulletins issued from Sarvodaya's Hazard Information Hub.

For testing purposes the LM-HWS was to design to replicate the components of the typical NEWS; i.e. a system equivalent to an end-to-end early warning system excluding the "detection and modeling system", illustrated in fig 1. The reader can map the components in Fig 2 to the subsystems in Fig 1 using the color scheme used to exemplify the identities. For research purposes the closed user group based system illustrated in Fig 2 will provide the identical functions of the NEWS, which is an aggregate of the National and Last-Mile Systems. Hence, the model in Fig 2 is an ideal replica to test the functional performance of envisaged NEWS.

A simplified information flow for the LM-HWS is as follows: staff members at the HIH monitor hazard events around-the-clock using the Internet. When a potential threat is detected, the HIH activates its Emergency Response Plan (ERP) by addressing a message to the n-number of communities at risk using a combination of wireless ICTs to reach local first responders (denoted by the yellow double headed arrow between the HIH and ICT-G blocks in Fig. 1). Each community has assigned a person or persons to be responsible for managing the wireless device and monitoring it for incoming warning messages. This person has received training from Sarvodaya and is designated as a community ICT-Guardian (ICT-G). When the ICT-G receives a warning message at the HIH, they are responsible for activating the community-level ERP. The community response will vary depending on the content of the message,

[3] The Lanka Jatika Sarvodaya Shramadana Sangamaya (Sarvodaya) is Sri Lanka's largest and most broadly embedded people's organization, with a network covering: 15,000 villages; http://www.sarvodaya.org/about. The 32 Selected Sarvodaya Communities were affected by the December 2004 Indian Ocean Tsunami and uniformly represent the 10 Tsunami affected Coastal Districts of Sri Lanka. These Communities also represent the different ethnic communities in the country.

including its priority level. During activation, the ICT-G informs the m-number of ERP Coordinators (ERP-C), consisting of a First-Aid team, Evacuation team, Security team, and Message Dissemination team. The Message Dissemination team then relays the message village-wide through various methods, including as word-of-mouth, ringing local temple bells, loudspeaker, and so forth

Message content is encoded using Common Alerting Protocol (CAP), an open source data interchange standard that includes numerous fields intended to provide consistent and complete messages across different technologies.[4] The implementation of CAP in the LM-HWS is an important aspect of the project because it is key in establishing an "all-media" warning capability. Section V describes the implementation strategy of CAP in Sri Lanka.

III. CALCULATING RELIABILITY OF ALERTING PROCESSES

The basic question governing the reliability measure is "did the ICT based system work on the day of the live-exercise?" Reliability, denoted by R can be measured in at least two aspects: *certainty* and *efficiency*; denoted by R_c and R_e respectively. Whereas certainty refers to the operational state of a device on the day of the exercise, efficiency measures the time taken to complete the transmission of a message in relation to the anticipated hazard risk (i.e., will the message be received with enough advance warning to take action?).

Using equations (2) and (3), the overall reliability R of the wireless ICT in a LM-HWS is computed as functions of the certainty and efficiency of the ICTs; where:

$$R = R_c \times R_e \qquad (1)$$

A. Certainty of Message Receipt

In some situations the ICT failed on the day of the exercise and was given a reliability score of 0 in terms of certainty. It was evident that the strength of the signal coverage was catalyst to an ICT-G undoubtedly receiving an alert. Signal coverage measures the certainty of a message reaching an ICT-G recipient at various times of day and is intended to reflect the variability between mobile, nomadic, and fixed wireless devices. Signal strength is important for the Alerting feature because if the signal is weak then some data can get lost. As a result the terminal device may not get the full bit string, causing failure to activate some of its active alerting function sensory features that are triggered by designated bits in the data string.

Wireless signal is usually measured as a function of the power of the signal in decibels (dB) then referenced to 1 mill watt (dBm) [2]. The signal strength was measured at the ICT-Gs home or the location where equipment was installed. A GSM mobile phone can function on -104 to -47 dBm range, Satellites operates on -127 to -60 dBm range, and CDMA phone operates on -106 to -48 dBm range. All the devices used in the project display their signal strength using illumination of histogram bars (or LEDs) that are a function relative to the dBm range of the device.

Given the device has a total of $y_{\max}$ bars, at a particular location such as the ICT-G's home, the device may have $y \leq y_{\max}$ number of bars illuminated; where y is a real number. For example, a particular terminal device may have the bars color coded; where a green bar implies full strength, amber bar implies half strength, and red bar implies zero strength. With such a color coding, a device with a maximum of 5 bars having 2 green bars, 1 amber bar, and 2 red bars illuminated may imply $y = 2.5$. For a particular application of the ICT (e.g. application of sending and receiving SMS) to work properly the service provider can specify a minimum requirement for the signal strength (such as 1 bar). Let us denote this minimum strength by $y_{\min}$. The device is given a score based on the signal strength indicated by the bars by applying the following formula:

$$R_c = \begin{cases} 1 / \left(1 + e^{y_{\min} - y}\right) & , y \geq y_{\min} \\ 0 & , y < y_{\min} \end{cases} \qquad (2)$$

The exponential function defined in (5) will give a score between 0 and 1. When $y = y_{\min}$ the score will be 0.5, implying that with the terminal device indicating minimum signal strength there is only a 50% chance that the alert message will come through without any doubt. As the number of bar $y > y_{\min}$ increase the score will reach a value of 1 at an exponential rate. Similarly as the number of bars decrease below the minimum number of bars needed the probability of receiving the alert drops below 50%. The calculation takes in to consideration that $y_{\max} - y_{\min} \approx 5$ because all of the ICT terminal devices tested in this project had either a 5 bar or 7 bar signal strength display; where all of the devices with 5 bars required approximately minimum application specific requirement of 2 bars and the devices with a 7 bar display required approximately a 3 bar minimum requirement. It is evident that the signal strength scoring equation (5) has to be refined and generalized for all ICT terminal devices. For the purpose of this research

[4] Botterell, Art and Addams-Moring, Ronja. (2007). Public warning in the networked age: open standards to the rescue. *Communications of the ACM*, 30 (7), 59-60.

equation (2) was sufficient. The authors recognize that equation (2) does not taken in to considerations of uncertainties caused due to operator (human) mishaps that are discussed in Section VI A.

B. Efficiency of Message Transmission

In conventional analysis, probability of efficiency requires a large amount of data gathered from multiple trials, a luxury the HazInfo project does not have. Therefore, the project used the methodology proposed in [6], which provides means to quantify R_e using Mean-Time-To-Failure (MTTF) with a single set of data. MTTF is a measure of expected time where the process will fail. Hence, reliability, in terms of efficiency, is defined as $R_e = 1 - MTTF$. The reliability: R_e measure would consider the aggregate of the time it took the HIH to transmit and alert message to the ICT-G and the time an ERP-C spent on activating the ERP at the community level, where Fig. 2 illustrates the communication architecture and Section II briefly describes the work flows.

Let us denote the time period of the message transmission processes with variable $\overline{T}$. An assumption is made that these processes must be completed by a benchmark time; i.e. expected time $E(\overline{T})$ because it is realistically impossible to complete a process in 0 (zero) time. Define the "hazard-duration" to be the difference between the hazard initiating time and the hazard impacting time, denoted by the variable T. The reliability: R_e of an exercise is calculated using the following formula:

$$R_e = 1 - \left(\frac{\overline{T} - E(\overline{T})}{T} \right) \qquad (3).$$

when $\overline{T} > E(\overline{T})$; otherwise $R_e = 1$ because the process was completed prior to the benchmark time. Similarly, the other extreme is if $\overline{T} > T$, then $R_e = 0$ because the time has surpassed the maximum allowable time; i.e. hazard-duration. Since this research is first of its kind and the live-exercises conducted in Sri Lanka was the initial set of tests. Therefore, an assumption was made to set the benchmark value to the best case scenario $E(\overline{T}) = 0$ (although humanly impossible for initial evaluation). In the future $E(\overline{T})$ can be estimated using previous sets of data such as the data collected during the live-exercise conducted between November 2006 and May 2007 in the HazInfo project live-exercises.

IV EFFECTIVENESS OF TERMINALS IN THE LAST-MILE

Effectiveness was measured as a function of a set of discrete parameters. The project has defined 11 such discrete parameters: language diversity, full CAP capability, audio and text medium availability, bi-directionality, total cost of ownership, DC power consumption, daily utilization, acknowledgement of message receipt, active alerting functionality, weight of wireless ICT, and volume of terminal device. Each parameter is denoted by a literal $q_1, q_2, \ldots, q_{11}$. A "Liken" type rating is used to obtain a real valued score between 0 and 1 for each literal, which is denoted by $P(q_i)$ for $i = 1 \ldots 11$. A conjunction of the literals $q_1 \wedge q_2 \wedge \ldots \wedge q_{11}$ defines the design requirement for an effective ICT in a LM-HWS. Hence, a single score for the effectiveness G of the deployed wireless ICT configuration is obtained by multiplying the real valued score of all the literals, as stated in equation (4).

$$G = G(q_1) \times G(q_2) \times \ldots \times G(q_{11}) \qquad (4)$$

The 11 parameters are further grouped in to 5 cliques: CAP Completeness, Two-way, Adoptability, Miniaturization, and Alerting; as shown in Table 1, which is not listed in any particular order as their contribution to effectiveness in a LM-HWS is equally important.

TABLE 1
CLIQUES AND THE SET OF CORRESPONDING PARAMETERS

Clique	Parameter
Adoptability	Daily utilization
	Total cost of ownership
Alerting	Acknowledgement of message receipt
	Active alerting function
CAP Complete	Language diversity
	Full CAP capability
	Audio and Text mediums
Miniaturization	Weight of wireless ICT
	Volume of wireless ICT
	DC power consumption
Two-way	Bi-directionality

A subset of the mentioned parameters (language diversity, full CAP capability, and audio/text medium availability), which defines the aspect of being *CAP Complete*, is already discussed in [9]. Equally important feature: *Alerting* capability of wireless ICT terminal devices, replying on the basis of the parameters: acknowledgement of message receipt and active alerting function is discussed in [11]. *Two-way* is an indicator to measure the ability of the device to permit upstream communications from local communities to the message Relay as well as downstream communication from the Message Relay to the Communities. The upstream communication is mainly for Last-Mile Communities to inquire-of and report situations affecting their communities. The MOP allows both upstream and downstream communication without any restriction. The RAD has limited the upstream communication such that the “call back” feature is operational only when an alert is received. Terminal devices must be affordable as well as have a utility in the last-mile communities. The *Adoptability* clique of parameters: daily utilization and total cost of ownership determined the effectiveness of the community’s ability to adopt the terminal devices into their daily lives in order for the device to be always on and is always used. The wireless terminal devices are used not only for disaster mitigation but also during relief and recovery periods. Therefore, the researchers emphasized that the Terminal devices be portable and could be easily installed and made operational in a nominal time period. The weight and volume parameter effectiveness measures are proportional to the ability of a single human being physically transport the units to any location. Operational time (longevity) of the device in an infrastructure free environment is reliant on the DC power carrying-capacity as well as the rate at which electricity is consumed. The three effectiveness measuring parameters: weight of ICT terminal, volume of ICT terminal, and DC power consumption together define the clique labeled as *Miniaturization*.

ambiguity in the alerts (for example, if the message indicates that the particular community is at no threat, then the community plan should be simply to acknowledge and record the message and do not relay it any further).

B. CAP Profile for Sri Lanka

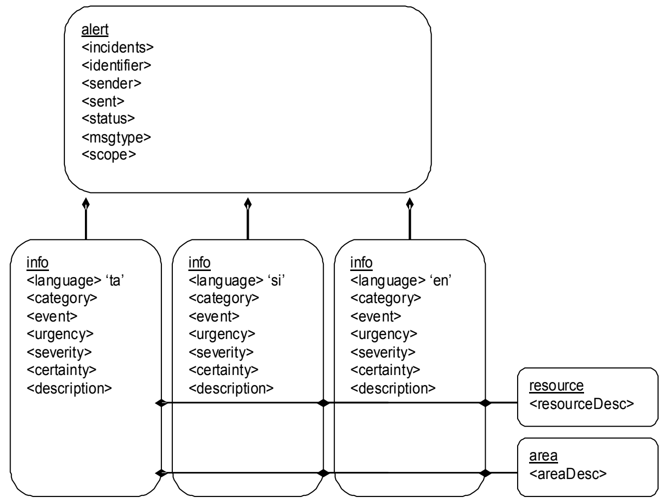


Fig. 3 - CAP Message Profile defined for Sri Lanka

V. CONTENT STANDARD TO TEST THE PERFORMANCE

A. Why use CAP

CAP was integrated into the project because of the following perceived benefits and advantages: it is an open source formulation, XML-based protocol with clearly defined elements, supports data interchange across multiple dissemination channels, with one input at the central information hub the message can be translated into multiple outputs for downstream alerting, provides a standardized template for submitting observations to the central hub (upstream) supporting situational awareness to improve overall management of a critical incident, and more easily integrate with other national and international information systems.

CAP standardizes the content of alerts and notifications across all hazards, including law enforcement and public safety as well as natural hazards such as severe weather, fires, earthquakes, and tsunami. This paper will specifically discuss the research findings of using CAP in a Multilanguage environment (Sinahala, Tamil, and English).

Designers of CAP (Botterell et al 2005), have given the message recipients full autonomy to take action based on the information they receive. It is expected that the community has an ERP that is executed on the basis of the content in the CAP message. Therefore, it is important to avoid

CAP, as described in [4], adopts a Document Type Definition (DTD) Extensible Markup Language (XML) data structure that consist of a main element <Alert> and subelements <Info>, <Area>, and <Resources> as illustrated in Fig. 3.

<*urgency*> Code that denotes the time to impact of the event. <*severity*> Code that denotes the scale of impact of the event. <*certainty*> Code that denotes the probability of the event. These 3 elements define the Priority of the <*event*>. The Priority is a higher order function that maps Urgency, Severity, and Certainty values to a distinct Priority: Urgent, High, Medium, or Low. The mapping is discussed in Table 2.

TABLE 2
MATRIX TO DETERMINE MESSAGE PRIORITY WITH CAP ELEMENTS

Priority	***<urgency>***	***<severity>***	***<certainty>***
Urgent	Immediate	Extreme	Observed
High	Expected	Severe	Observed
Medium	Expected	Moderate	Observed
Low	Expected	Unknown	Likely

“*CAP Message Interoperability*” was subjectively studied by assessing the “action taken” by the message recipient. For this assessment, the CAP message relayed from the HIH and actions taken were recorded by each First-Responder. The effectiveness was measured as to how well the First-

Responders could record the message received over the particular device and interpreted.

VI. EXPECTED PERFROMANCE OF THE DEVICES

A. Remote Alarm Device

RAD is based entirely on widely available mobile communications technologies Short Messages (SMS) and Cell Broadcast Messages (CBM). SMS Based alerting is used to activate selected or individual RADs, while the CBM is used to activate all RADs. These terminal devices are stand-alone units that incorporate remotely activated alarms, flashing lights, a broadcast FM radio receiver to be turned off or on as directed by the message, the displaying of the SMS messages on LCD panel, a self-test button, message acknowledgement and a dynamic hotline GSM call-back feature for user to acquire additional information. Five push button switches labeled as Call, Ack, LCD, Test, and Radio control the operational states of the device. The GSM Alarm Device is a product of the University of Moratuwa Dialog[5] Communication Research Lab [3].

The Microcontroller and the GSM module are the key components of the Alarm Device. The microcontroller houses a multitude of peripheral devices such as internal program flash memory, Data Memory, general purpose I/O, and USARTS. Once in operation, the GSM module listens for any incoming SMS messages or CBMs. CBM-based warning messages will be broadcast on a predetermined dedicated logical broadcast channel. Upon the reception of a CBM or an SMS, a notification will be sent by the GSM module to the microcontroller. The Microcontroller in turn will read and processes the message. If the message is from an authorized source (in case of SMS) and conforms to a given format the Alarm Device will be triggered. The RAD is designed to power up from the mains supply but is equipped with a seven hour back up battery as a secondary power source.

HazInfo project was the first to field test the RADs. Hence usability and effectiveness of the devices were questionable from the beginning. Having disregarded the issue faced by congestion in SMS applications the units were found to be exceptionally reliable during Lab tests. The external turning-indicator type flashing light used in vehicles and 40watt speaker ranked the RAD to be the unit to have the most forceful active alerting functions. The 160 character limited display designed for English text messaging only established the device to have very low effectiveness. Since the GSM signals cover only 60% of Sri Lanka the units would be limited to locations with good signal coverage. The sets had absolutely no value addition to integrating them in to the village daily life, reducing the effectiveness scores further.

[5] Dialog Telekom url on the Disaster and Emergency Warning Network – http://www.dialog.lk/en/corporate/cr/ourapproach/innovationinclusion/dewn.html

B. Mobile Phone

The research used Nokia 6600 MOP that are powered by a 104MHz ARM processor, and is based around Symbian's Series 60 platform. Microimage[6] developed a J2ME applet that sits on Symbian Operating System. The MOPs are activated by a SMS sent from an Internet Application that can be configured to send alerts to all or a group of MOP handsets. The GSM Java enabled SMS mobile phones receive text alerts in Sinhala, Tamil and English, sounds an alarm, and has a hotline GSM call-back feature.

Given that the MOP had a java based client software that fulfilled all three features of the active alerting function, as well as text messaging in all three national languages the devices was expected to perform the best with very high effectiveness. Since SMS messaging requires less signal strength opposed to voice the MOP based solution was, further, trusted to be highly effective. The ubiquitous technology with a device that can be alongside the ICT-G at all times and could be easily integrated in to their daily village life would prove to be most reliable device of the lot.

C. Operational States of the GSM devices

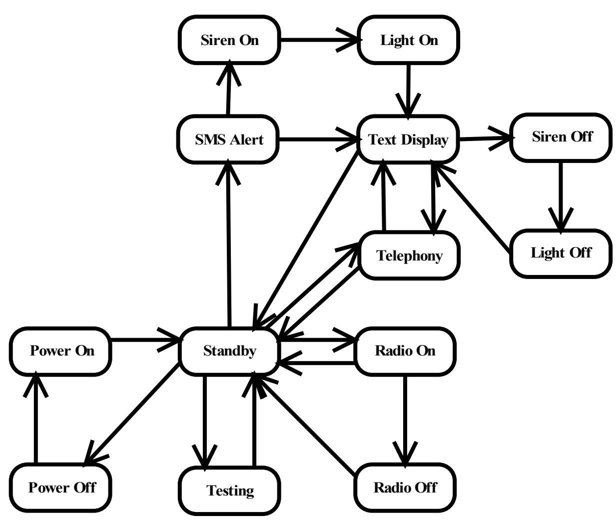


Figure 4 - expected operational states of the RAD & MOP

Power On -- the RAD is powered by 240v 60Hz AC and when the main power is down it is run by a Matrix 7v DC Lithium Battery. The Nokia 6600 has a rechargeable 9v Battery. At this point the GSM Module in both devices

[6] Microimage website – http://www.microimage.com

listen to SMS of the type that are Alerts and be on *Standby*. SMS Alert is a specific SMS with a known header that triggers the device to initiate the Alerting Sequence. The total message is the size of 2 SMS messages; i.e. 2 x 140 7bit characters. *Siren On*, *Light On*, and *Text Display* are instantaneous. The User can press the "Acknowledge button" to turn the *Siren Off* and *Light off*. The User then uses GSM *Telephony* by pressing the "Callback button" to dial the Alert Sender for direct conversation or to receive a voicemail of the CAP message. Final step is pressing the *Radio On* to listen to an FM Emergency Broadcast Station (not available in the Nokia 6600). This completes the cycle of operational states of the 2 GSM based Terminal devices.

D. Encoding and Transmission of CAP Messages

CAP message is entered via an Internet based application: Disaster and Emergency Warning Network (DEWN); namely a HTTP Software Application. The HTTP server strips the <*msgType*> and <*description*> elements of the CAP message. The data is then transformed and packed in to 2 SMS packets and delivers to the Short Message Service Controller (SMSC). This truncated CAP message is then forwarded to the GSM Terminating device: RAD or MOP via the Dialog GSM network.

E. Reception and Decoding of CAP Messages

The first 140 character 8 bit special SMS text message contains a header code of 10 characters, which is decoded by the RAD's Microcontroller and by the MOP's J2ME Applet. Remaining 130 characters contain the text message taken from the <msgType> and <description> of the orginal CAP message. The software in the devices activates the alarms of the devices and display the text tripped from the specially encoded SMS packets. The RADs displays only the English portion of the text message; where as the MOPs display the Sinhala, Tamil, and English text messages.

VII. OUTCOME OF DEVICES IN FIELD TRIALS

A. Uncertainty and Inefficiencies in Messaging

The terminal device reliability measures: certainty and efficiency were recorded on the day of the live-exercises. The results in Fig. 5 are a summary (average) of the measures obtained during each of the exercises conducted in the individual communities.

Certainty in the RAD devices dropped below a benchmark of 0.85 because the signal strength in location of the devices measured between 2 – 3 bars. However, this did

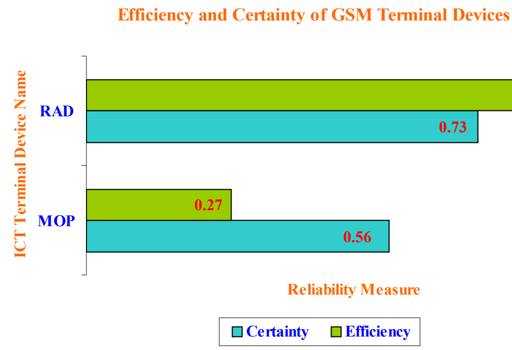


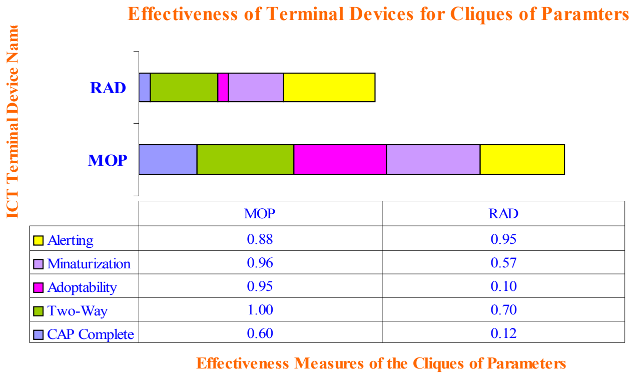
Fig. 5 - Certainty and efficiency

not effect the SMS alert coming through because 1 bar was sufficient to receive the alerts and activate the alerting operational states of the device. The research experienced cases of 0 (zero) certainty due to unquantifiable reasons where the community ICT-G had accidentally deleted the J2ME applet, had forgotten to charge the battery of the MOP, had not paid the phone bill, communities in the North and East conflict areas of Sri Lanka being denied GSM access because the Government of Sri Lanka was conducting military operations and had instructed the mobile operators turn of the cells in those conflict areas.

In some communities the alert message was not received during the first attempt of pushing the messages to the MOPs using the DEWN Internet application. Therefore, the efficiency dropped as a result of excess time taken to repeat the process in order for the MOPs to receive the alerts.

Normally both GSM devices take less than 30 seconds to push the alert messages to the end user devices. No more that 1 – 3 units were used during any given trial. Therefore the trials were not effected by congestion even thought both solutions use a store-and-forward method to push the SMS alerts to each device. Ten MOPs were tested in the different communities. Hence, the additional samples used in the trials compared to the 2 RAD units used the research had the opportunity to learn lessons of unsuccessful behaviors. The MOPs tested in the rural environments, where the ICT incompetence of the ICT-G in the communities using non traditional feature introduced by inserting a J2ME applet, for example, further effected to the efficiencies because the menu and instructions were in English, incomprehensible by folks in the rural areas. The RAD score a high rating in terms efficiency because only 2 units were used in the field trials and they both happened to performed quite well in the urban environment. The distinctly marked 4 buttons in he RAD opposed to the menu driven MOP simplified the transition between operating states to increase efficiencies.

B. *Effectiveness of Alerting the ICT-G*



	MOP	RAD
Alerting	0.88	0.95
Minaturization	0.96	0.57
Adoptability	0.95	0.10
Two-Way	1.00	0.70
CAP Complete	0.60	0.12

Fig. 6 – Effectiveness measured for each Clique

Both units, the RAD and MOP, have good active alerting capabilities because they both have audible sirens and a flashing light. The MOP can be weak at times when the device is conceiled in a trouser pocket or is ditached from the ICT-G at a distance; where both the audible siren and light may not be strong enough to get immediate attention of the ICT-G. However, the RAD is the most effective unit of all the ICTs tested. The RAD would gain the immediate attention of the ICT-G as a result of the loud siren and externaly mounted large orange light even from a distance of 50 meters.

Of the two units the MOP has the best Miniaturization features; where the ICT-G can carry the MOP, weighing less than 200 grams (Nokia 6600 weighs 130 grams), in an external belt-case or the pocket, whcich also frees their hands. Comparitively, the weight and size of the RAD requires a single person to carry the unit by its fixed handle or, as an alternative, carry the RAD in a backpack. The RAD works both on AC and DC power. However, the 12v battery that provides the power to the unit had approximately 4 hours or less of a life time, when the unit went through all the operational sates in receiving multiplicity of repeated alerts . Unlike the MOP, which is quite versatile, the RAD does not provide utilities other than the FM radio and for alerting for the average citizen to use in their daily lives. The initial design of the units were for Government First-Responders; where the sets telephony feature of the unit was denied. Therefore, the community users were not able to use the unit to make voice calls or send SMS as an when they wanted, restricting upstream comunication. The voice call was active as a ‘call-back” feature only following the receipt of and alert; where the user would press a button to call back a central information source at a pre programmed phone number. The restriction in two-way comunication in the RAD ranked very low compared to the MOP, which was unrestricted. In regards to CAP Completeness, ony the MOP was capable of receiving messages in the three languages: Sinahala, Tamil, and English. The RAD was capable of receiving Englishe text messages.

C. *Shortcomings of the ICTs with the use of CAP*

The 2 GSM ICTs used in the project make use of the CAP message format. As illustrated in Table 3, each is only capable of displaying a limited number of the CAP elements, limiting the amount of alert message content that can be transmitted to the ICT-G. Consequently, during simulations, ICT-G recorded only the *<msgType>* and a truncated portion of the *<description>* elements because that’s all they received. Although, the RAD and MOP devices use the *<description>* element that could have carried a complete set of information, they were restricted to an overall message content limit of 270 characters, which is insufficient to carry a meaningful unambiguous alert message. Message did not include *<urgency>*, *<severity>*, and *<certainty>* to enable ICT-Guardians to judge the *Priority* of the incident, which is mandatory for the CAP Profile for Sri Lanka. Therefore, both devices were only good for getting the attention of the ICT-G that there was an eminant threat but were forced to seek complete information from an alternate source.

Example 1: The simulations began at the HIH with the receipt of an email containing the critical information pertaining to a Cyclone hazard. The following abstract of the entire message contains the critical information of the message.

> “A SEVERE CATEGORY 4 CYCLONE is now current for HAMBANTOTA District coastal areas. At 10:00 am local time SEVERE TROPICAL CYCLONE MONTY was estimated to be 80 kilometers west of Hambantota and moving southeast at 10 kilometers per hour.”

The HIH then transformed message to a CAP Message and entered the relevant information in to the DEWN HTTP application. The *<msgType>* was set to “Warning” and the Cyclone message was inserted in to the *<description>* field. The Cyclone message was translated to Sinahala and Tamil languages to be used; especially with the MOP.

Table 3 illustrates the elements of the CAP message received and parts of the message received by each of the devices. The RAD provided more information than the MOP but no a full message where it was truncated after 160 characters. The MOP displayed that there was a Cyclone warning in effect but had no additional information as to where and when the hazard is effective.

TABLE 3
MESSAGES RECEIVED BY THE RAD AND MOP

RAD	***MOP***
"Warning A SEVERE CATEGORY 4 CYCLONE is now current for HAMBANTOTA District coastal areas. At 10:00 am local time SEVERE TROPICAL CYCLONE MONTY was estimated to be 80 kilometers west of Hamban"	"Warning" "A SEVERE CATEGORY 4 CYCLONE" " {same in Sinhala}" " {same in Tamil"

VIII. CONCLUSION

Cell Broadcasting solves the congestion problem faced in SMS. However, it will not be affective for public alerting unless it can provide a Complete Full CAP Message with proper instructions and unambiguous messages. Until then it is recommended that the experimented SMS based technologies be used with capabilities to actively alert the ICT-G; where the ICT-G is expected to seek further information by listening to a radio or TV broadcast or other reliable means. The field trials observed when proper information is not provided to the ICT-G the communities executed the wrong ERPs. As it was the case when a Cyclone alert was issued the communities executed a Tsunami evacuation drill, which involved running to hire grounds when they actually should have sought shelter in lower grounds. Research conducted by Y. Fu et al (2007 August) also exemplifies the repercussions of false information propagation during emergency situations [13].

The 2 GSM devices used in the HazInfo Pilot cannot be upgraded to receive Complete Full CAP Messages and will never score a value 1.0 because of the restrictions posed by the Terminal Devices. However, could score an effectiveness value of, at most, 0.80. This is achieved by strictly using the *<event>*, *<urgency>*, *<severity>*, and <certainty> elements of the *<info>* section in a single 8 bit 140 character SMS or 8 bit 93 character CB message instead of using the *<description>* element of the CAP messaging structure. One of the 8 bit characters can be used to enumerate the combination of *<urgency>*, *<severity>*, and *<certainty>* to determine the Priority. This would require mobile phone manufacturers of third party software companies to develop software that can be preinstalled in the devices. The pre installed software would to decode the the enumerated bits to determine the text to display corresponding to the *<urgency>*, *<severity>*, and <certainty> elements in the user identified language. Thereafter, the remaining characters of the SMS or CB message can be used to carry the <event> information, which will be sufficient in length to carry an unambiguous alert message in the last-mile languages at the first alerting instance before network congestions starts and all GSM means of communication such as GPRS, Voice, and SMS will cease. Further, coupling GSM Mobile devices with FM radios have proven to be highly effective for receiving emergency broadcasts during the critical hour when congestion takes place.

REFERNCE

[1] Anderson, Peter (2006) Last of the Mile Warning System ICT *Assessment and Community Simulation Observation Report*, LIRNEasia HazInfo Project [available from author – anderson@sfu.ca]

[2] A. Beresnev "Measuring Devices and Methods for Analysis of Coverage Area in GSM Cellular Systems, IEEE Conference on Electron Devices and Materials, Thomsk State University of Control Systems and Radioelecronics, Tomsk, Rassia. Paper can be obtained from author – san@tcc.tomsk.ru (Published)

[3] Dias, Dileeka, Jayasinghe, Gamini, Fahmy, Farazy, Galaweera, Nuwan (ICIIS 2006). A GSM Alarm Device for Disaster Early Warning. Proceedings of the *First International Conference on Industrial and Information Systems*, Peradeniya, Sri Lanka. (Published)

[4] G. Gow (2007 March/April). Implementing Common Alerting Protocol for Hazard Warning in Sri Lanka, *Journal of Emergency Management*, Volume 5, Number 1, pages 50-56

[5] J. Chesterfield, P. Rodriguez, (2003). DeltaCast: Effetient File Reconciliation in Wireless Broadcast systems. Paper available here -- http://research.microsoft.com/~pablo/papers/deltacast_mobisys.pdf

[6] Othman, Zalinda, Subari, Khairanum, Morad, Norashima, Applications of Fuzz Inference Systems and Genetic Algorithms in Integrated Process Planning and Scheduling www.journal.au.edu/ijcim/2002/may02/article5.doc

[7] Samarajiva, Rohan. (2005). Mobilizing information and communications technologies for effective disaster warning: lessons from the 2004 tsunami. *New Media and Society*, 7 (6), 731-747.

[8] Samarajiva, Rohan, Knight-John, Malathy, Anderson, Peter, Zainudeen, Ayesha et al. (2005, March 17). National Early Warning System Sri Lanka: A *Participatory Concept Paper for the Design of an Effective All Hazard Public Warning System* Version 2.1, LIRNEasia and Vanguard Foundation, 2006. Available http://www.lirneasia.net/projects/completed-projects/national-early-warning-system/

[9] N. Waidyanatha, G. Gow, P. Anderson (May 2007). Hazard Warnings in Sri Lanka: Challenges of Internetworking with Common Alerting Protocol, *Proceedings ISCRAM2007 (B. Van de Walle, P. Burghardt, and C. Nieuwenhuis, eds.)*, Pages 281-293. Paper can be found here -- http://www.iscram.org/dmdocuments/ISCRAM2007/Proceedings/Pages_281_293_40DSM_07_A_Hazard.pdf

[10] N. Waidyanatha, G. Gow, P. Anderson (2007 August). "Common Alerting Protocol Message Broker for Last-Mile Hazard Warnings in Sri Lanka: An Essential Component". *Proceedings of the 2nd International ISCRAM Workshop, Harbin, China (B. Van de Walle, X. Li, and S. Zhang, eds.)*, Pages 59 - 65

[11] N. Waidyanatha, G. Gow, P. Anderson (2007 October). Community-based Hazard Warnings in Rural Sri Lanka: Performance of Alerting and Notification in a Last-Mile Message Relay, *Proceedings IEEE 1st International WRECOM2007 Conference and Exhibition, Rome, Italy*. (Published)

[12] N. Waidyanatha (2007 December). Last-Mile Hazard Warning System in Sri Lanka: Performance of the ICT First Responder

Training Regime, *Proceedings CPRsouth2 Conference, Chennai, India.* (In Press)

[13] Y. Fu, T. Liu, F. Zhu (2007 August). Scenario Simulation of Fake Information Diffusion in Pubic Crisis using Patterned Chaos Forecasting. *Proceedings of the 2nd International ISCRAM Workshop, Harbin, China (B. Van de Walle, X. Li, and S. Zhang, eds.)*, Pages 70 - 74

First N. Waidyanatha Past education experience includes a Master of Arts in Operations Research, Department of Mathematical Sciences, University of Montana, USA (Sept 1996 – May 1999) and a Bachelors of Arts degree in Mathematics with minor in Computer Engineering, University of Maine, USA (Jan 1990 – May 1995). The primary and secondary schooling was predominantly in Sri Lanka.

Nuwan Waidyanatha is currently the Project Manager of "Evaluating a Last-Mile Hazard Dissemination Research Project" for LIRNEasia in Sri Lanka. Nuwan is currently the Director of Spot On Solutions. He launched and developed Infocraft Limited contributing expertise in software engineering, management and operations research (Aug. '02 – Jan. 05). Worked as a Business Analyst for Sri Lanka Institute of Information Technology (Dec 2001 – July 2002). Career in the IT industry began with working as an Analyst Programmer for APS Healthcare and developing clinical/health manage care software solutions in USA (May 2000 - Nov. 2001). Other relevant experiences include being an Instructor in OR, Department of Mathematical Sciences, University of Montana, U.S.A. (Sept. 1999 - May 2000) and an Analyst Programmer, Montana World Trade Center, Montana, USA (May 1998 - Dec. 1998). More details www.lirneasia.net.

Second D. Dias, PhD Dileeka Dias has B.Sc.(Eng.) specializing in Electronic & Telecommunications Engineering from the University of Moratuwa, Sri Lanka, and an M.Sc and PhD. From the University of California, Davis. She is a Professor at the University of Moratuwa, and is the Dean of the Faculty of Information Technology. She specializes in wireless communications and is actively engaged in research and development activities in this area. She is also the Director of the Dialog Mobile Communications research Laboratory at the University of Moratuwa. For more details see http://www.ent.mrt.ac.lk/web/staff.xml

Third H. Purasinghe (CEO, Microimage) Harsha founded Microimage in 1993 at the age of 19. It was incorporated in 1995 as Microimage (Private) Limited. Harsha developed the company from a desktop language software provider to one of the leading innovative software development company in Sri Lanka with regional presence and global recognition to date. He posses over 10 years experience in mobile technologies. Harsha is the Chairman/Managing Director and CEO of Microimage with staff strength of 40 in Sri Lanka and Singapore. Harsha was recognized as the "Most outstanding entrepreneur in IT/BPO industry in Sri Lanka" recently. Today Microimage has transformed into a leading technology innovator where the company recently won the GSM Association Mobile Innovation Award in Asia and also received a commendation at the GSM Association global mobile awards in Barcelona, Spain. Further company to date has won many awards & recognition for its technology innovations such as National Science & Technology Award, BCS National Best Quality Software Awards for many years & featured in the interactive keynote delivered by Dr. Craig Barrett (Chairman Intel Corporation). The company holds patents and pending patents for some of its technological breakthrough's. For more details on the company visit (http://www.microimage.com).