eXtraordinary Message Service (XMS)

Martin DONOVAL, Bachelor Degree Programme (4)
FIIT STU Bratislava
E-mail: donoval@freeland.sk

Ladislav GAŽO, Bachelor Degree Programme (4)
FIIT STU Bratislava
E-mail: ladislav.gazo@szm.sk

Marek GREGOR, Bachelor Degree Programme (4)
FIIT STU Bratislava
E-mail: marek.gregor@zoznam.sk

Juraj OBERT, Bachelor Degree Programme (4)
FIIT STU Bratislava
E-mail: juraj.obert@centrum.sk

Supervised by: Mária Bieliková, PhD.

Keywords: XMS, Invisible Guardian, emergency service, personal guarding system

ABSTRACT

Nowadays it is not a surprise to get mugged during the day or kidnapped while walking home. The most significant and crucial action to be executed by the person being endangered is informing someone 'out there' with a message 'I need help'. As no appropriate support of getting help in most current situations for everybody existed so far, we proposed a novel concept based on a new message service called XMS (eXtraordinary Message Service). XMS allows people in danger to forward the responsibility of solving the situation to someone else. It extends the meaning of the word 'message' to include the only means for calling for help in situations where the usage of other ways of communication is limited or even impossible.

Concerning the way of delivery, the principle of XMS is similar to the well-known SMS (Short Message Service), but XMS provides some spectacular features that render the need for a new service inevitable:

- Highest priority reliable delivery service
- Device independence
- Status independence
- Special signaling for the recipient

First implementation of XMS is included in a system called Invisible Guardian. Invisible Guardian consists of two basic parts: a mobile device which serves as a communication gateway and sensors which represent the senses of the system. With correct indication, sensors are able to recognize a danger. They are placed on the human body or clothes and are wirelessly connected to the mobile device. The mobile

device software recognizes that a particular situation occurred (the user is not limited to one situation; the situation is determined by detecting corresponding activation procedure), composes an XMS message and sends it to the predefined recipients according to the delivery policy.

1 INTRODUCTION

Our first-rate aim is to deliver the possibility of calling for help in most current situations to everybody. In order to reach this goal we proposed a new message service called XMS (eXtraordinary Message Service) which is used to reliably deliver emergency messages. New message service is needed as no current messaging technologies are suitable for delivering such sensitive data as emergency messages are.

Current existing solutions are represented by systems such as Lifeline Personal Response Service [1], The CarePartner Communicator or 911 Mobile GPS Emergency Cell Phone [1] Lifeline Personal Response Service. http://www.easylivingprogram.com/pers.shtml. All of these products are based on the presumption of existing call centre, require subscriptions, are noticeable and are mostly dedicated to a restricted group of people. As opposed to this, XMS is designed for most current situations and its usage is not constrained by the existence of a call centre.

XMS is implemented in a system called INVISIBLE GUARDIAN which we designed to show how powerful the XMS can be. INVISIBLE GUARDIAN is a personal guarding system which utilizes XMS to inform about a danger. It consists of two basic parts: mobile device and sensors (as shown in Fig. 1). The **sensors** are placed on the human body and are able to recognize the danger with correct indication from the user. The person only has to perform simple, easy-to-remember and inconspicuous action. Such an

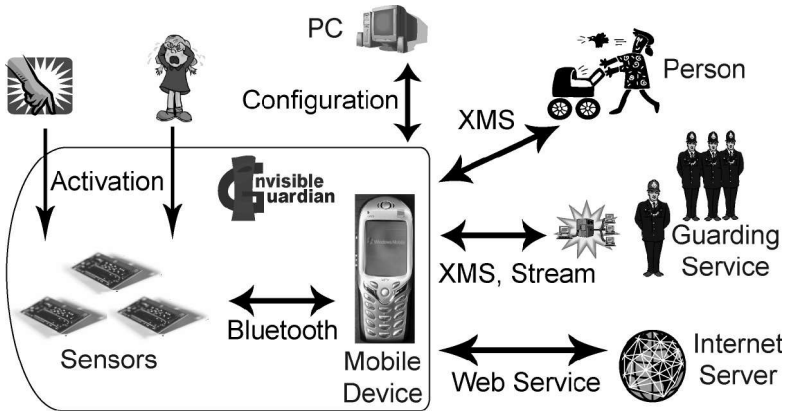

Fig. 1: System's context and data flows.

action is required as the system has to be usable in every situation where there is a chance that help will be needed. For example, the system may be used in situations of getting mugged or kidnapped. When a mugger shouts 'Put your hands up', the

endangered person says 'Don't hurt me', the voice sensor captures the speech and sends it to the mobile device.

The main task of the **mobile device** is processing the data coming from sensors, detecting dangerous situation and forwarding the information about the danger to persons or guarding services[1]. The software in the mobile device is configurable and allows the user to predefine the situation and specify the behavior for the case when the situation is detected. To sum up, providing that sensors act as the senses the mobile device acts as the brain. Different signals represent different situations so the user may set up the system to react differently to a number of situations. The reaction mainly specifies how to inform about the danger and whom. An important part of the XMS message is the location of the sender which provides significant help for organizing the rescue operation and increases its probability to succeed. Furthermore, the location awareness enables the usage of a developed web service which allows semiautomatic configuration of recipients based on current location.

2 XMS (EXTRAORDINARY MESSAGE SERVICE)

XMS is a new message service we proposed for delivering emergency messages. To give reasons for the need of a new service, we examined several considered alternatives (see Table 1).

Technology	Advantages	Disadvantages
SMS (Short Message Service)	+ Supported by majority of network operators + Supported in almost every mobile device	- Not reliable - Text-based (not extendable) - Overlookable
E-mail	+ Comfortable + Not text-based (MIME supported by many clients)	- Not reliable - Recipient needs to be online - Not supported in all mobile devices
GPRS	+ Reliable delivery + Flexible	- Recipient needs to be online - Not supported in all mobile devices

Tab. 1. XMS alternatives.

The summary in Table 1 implies several significant features that are inevitable for a desired message service and also highlights major issues connected with existing technologies. Most important features of XMS are:

HIGHEST PRIORITY RELIABLE DELIVERY SERVICE. XMS is supposed to be supported by network operators at the highest possible level of reliability, speed and priority.

DEVICE INDEPENDENCE. It is possible to implement the support for XMS into almost every mobile device that exists today – cell phones, PDAs or watches – the portability is ensured by network operators as the transport technology for XMS may

[1] Guarding Service – under this term we understand a public institution such as police or mountain rescue service

be GSM, CDMA, UTMS or any other operator's technology.

STATUS INDEPENDENCE. Low-level implementation of XMS in the mobile device allows the service to perform always when it is needed. A user playing Snake II, surfing the web, performing a call or writing an SMS **must be interrupted** to allow instant reaction to the incoming XMS message.

SPECIAL FEATURES. Instant access to key functions such as an audio stream request, acceptance/decline of the message is crucial in order to allow fast reaction of the user. The possibility to accept or decline the emergency message is crucial as the recipient does not have to be in a position to provide or arrange help for the sender. Another point is the way of signaling the message arrival – it **must not be overlookable** – all current technologies such as SMS or GPRS are overlookable.

2.1 XMS SPECIFICATION

Proposed format for XMS packets is shown in Fig. 2.

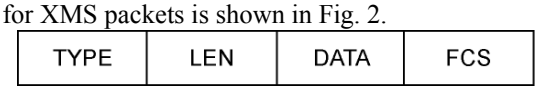

Fig. 2: General XMS packet format.

The TYPE field distinguishes between the following possible XMS packet formats:

- Help request – the initial XMS message packet format sent to request help,
- Help accept / decline – recipient's response to sender's help request,
- Stream request – recipient's request sent to the sender to request streaming,
- Stream accept / decline – sender's response to recipient's stream request,
- Recipient timeout – sender's indication that recipient's time to answer expired,
- Help / Stream cancel – cancellation messages for Help / Stream request messages,
- Update – indication that relevant data have changed (e.g. current location).

The LEN field stands for the length of the DATA field. The DATA field content depends on the TYPE field. In Fig. 3 we provide the packet format of the Help request message which is encapsulated in the DATA field. Table 2 contains description of the

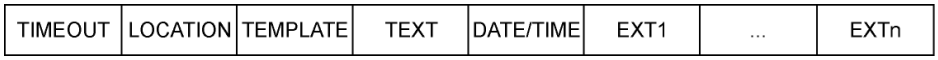

Fig. 3: Help request XMS message packet format.

fields involved.

Field	Meaning
TIMEOUT	The length of the time interval within which the recipient has to answer the help request
LOCATION	Current location of the sender
TEMPLATE	The kind of the detected situation
TEXT	Sender-defined text message

DATE/TIME	Date and time when the XMS message was sent
EXT1…EXTn	Sensor type specific fields – reserved for future sensor types

Tab. 2: Help request XMS message fields.

The behavior of the device implementing the XMS technology differs according to the role the device plays in the communication. We distinguish between the **sender** – a person who needs help and sends an XMS message and the **recipient** – a person or guarding service supposed to provide or arrange the help. The statechart diagram for the **sender** role is shown in Fig. 4.

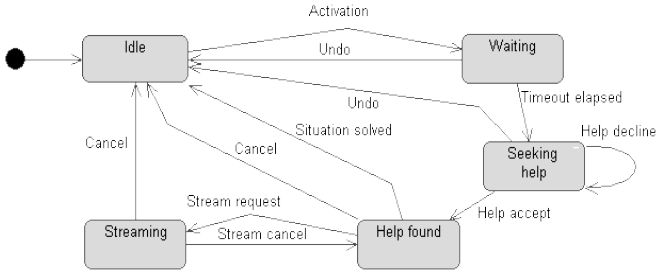

Fig. 4: Sender statechart diagram.

3 ARCHITECTURAL DESIGN

In order to demonstrate the capabilities of the XMS and to create a realization of the new concept of forwarding the responsibility in dangerous situations we designed and prototyped the INVISIBLE GUARDIAN system. INVISIBLE GUARDIAN employs two main parts to fulfill its functions: the mobile device and sensors. Also there are additional external software components which in conjunction with the INVISIBLE GUARDIAN and the XMS technology present a complete solution for handling dangerous situations. The deployment of the software components is illustrated in Fig. 5.

The basic data the system works with are received from sensors. When the user performs an action with the sensor (e.g. drawing V-shaped symbol on a touchpad sensor) the data are captured by the sensor, preprocessed within it and transmitted to the mobile device. The mobile device software determines if a known event happened by comparing interpreted received data to defined activation procedures. If this is the case, an XMS message is built according to the configuration (this may require gathering additional data from sensors, e.g. current location from the GPS sensor) and particular component of the mobile device software is asked to deliver it. XMS messages are delivered to the recipients in the one-by-one manner while waiting a specified amount of time for each recipient to answer. Upon successful acceptance of the XMS message by the recipient additional functionality such as streaming may be requested.

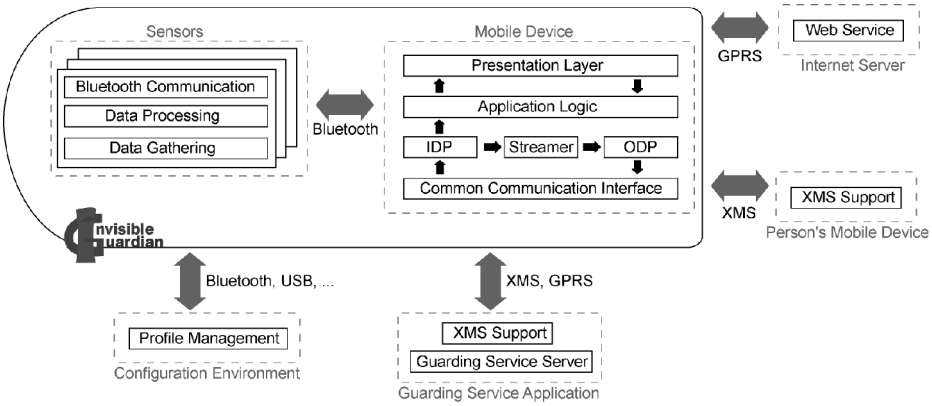

Fig. 5: Software deployment and architecture.

3.1 SENSORS

The main tasks of sensors are capturing, preprocessing and transmitting the data to the mobile device wirelessly. The hardware design of a sensor is shown in Fig. 6.

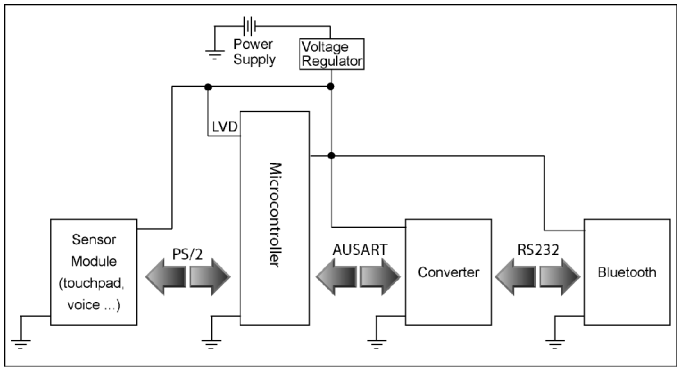

Fig. 6: Sensor hardware design.

The hardware design fulfills the following design objectives we have set: small size, low power consumption and low battery detection.

Every sensor consists of four main components. The only sensor type dependent component is the sensor module – which captures the input data from the user (e.g. strokes, voice) – and partially the software of the PIC microcontroller – which preprocesses the captured data. The Bluetooth module and the Converter are sensor type independent. The program running in the PIC microcontroller is completely interrupt-driven to ensure the possibility of processing the data from the Sensor Module and the Bluetooth Module.

3.2 ;MOBILE DEVICE SOFTWARE

The main tasks of the mobile device software may be summarized in the following points:

- communication with installed sensors and the outer world,
- analysis of the data received from sensors and event recognition,
- building and delivering XMS messages and data streaming,
- access to web services and providing the user with a configuration environment.

The architecture of the mobile device software is shown in Fig. 7 (arrows in the picture depict data flows).

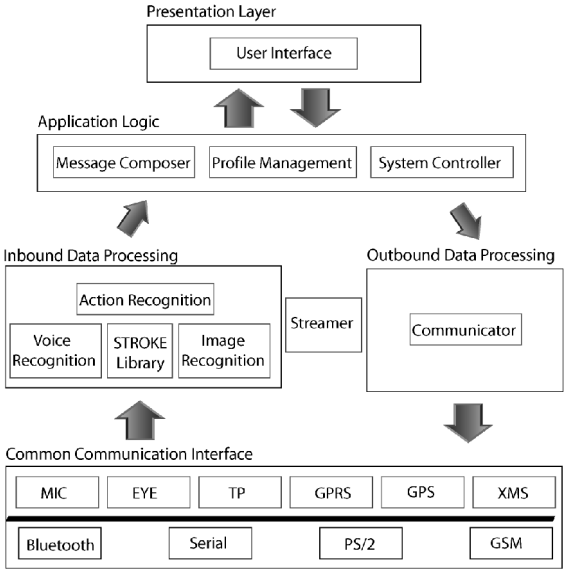

Fig. 7: Architecture of the mobile device software.

The bottom layer is responsible for providing communication between the mobile device and other devices – sensors, cell phones, etc. using various technologies such as Bluetooth or GSM. It is also responsible for providing interpretation logic for each sensor type (MIC, EYE and TP components in Fig. 7) and encapsulation capabilities for higher-level protocols – XMS or GPRS.

The middle layer is divided into two parts responsible for processing inbound and outbound data separately. The Inbound Data Processing part provides mechanisms for analyzing the data captured by sensors and transmitted to the mobile device. It contains recognition engines for each sensor type which provide inputs for the action recognition component – the first component able to identify that a particular event happened.

The Outbound Data Processing part handles all data coming out of the system. These are mostly XMS messages, data streams, sensor control commands or access to web services. As the architecture model indicates, by employing the services of the only component of the Output Data Processing part – the Communicator – it is possible to route the outbound data through any communication interface which has a driver at the CCI layer.

The Application Logic layer handles the following main tasks: message composition, behavior logic, system control, profile management and access to web services. The Application Logic layer is the very brain of the system which controls all its components. The Streamer is a bridge between the Inbound Data Processing and the Outbound Data Processing parts. It allows streaming of live data from sensors by placing itself between the interpreted input from sensors and the output delivery mechanism – the Communicator.

The Presentation Layer provides the user with a configuration environment allowing him/her to customize the system using the mobile device only.

4 SUMMARY

We proposed a new concept of forwarding the responsibility in dangerous situations based on a new message service called XMS (eXtraordinary Message Service). The focus is on the word eXtraordinary – situations such as mugging or kidnapping are definitely of that kind and at present there has been no known technology for handling them. An obvious example: one may try to send an SMS message when kidnapped but who guarantees the delivery? No one does. Moreover, it is quite impossible to compose an SMS message without attracting attention of surrounding people.

We implemented the support for XMS in the INVISIBLE GUARDIAN system – a guarding system based on a collection of sensors placed on a human body or clothes and a mobile device. It allows the user to perform an inconspicuous action to inform about danger – using the XMS technology the mobile device sends an emergency message to predefined recipients that are asked to provide or arrange help.

Although the primary scenario for using INVISIBLE GUARDIAN is street crime, it is important to emphasize that there are also other scenarios where the usage of INVISIBLE GUARDIAN is applicable e.g. health hazard or stressful situations (such as being lost).

INVISIBLE GUARDIAN is not be confused with a monitoring system as all functions it performs are controlled by the user and no private information are provided to third parties without user's explicit approval.

To sum up, the combination of XMS and INVISIBLE GUARDIAN presents a complex solution for handling dangerous situations providing unified communication technology for delivering emergency messages and invisible user-friendly guarding system for detecting the danger. It is a computer-based system solving one of the most socially valuable problems – the problem of limited possibility of calling for help in dangerous situations.

5 REFERENCES

[1] Lifeline Personal Response Service.
`http://www.easylivingprogram.com/pers.shtml`

[2] 911 Mobile GPS Emergency Cell Phone.
http://www.safetyandsecuritycenter.com/mogpsemph.html