Ingeniería Investigación y Tecnología. Vol.XI. Núm.2. 2010 217-231, ISSN1405-7743 FI-UNAM
(artículo arbitrado)

Generic Model to Send Secure Alerts for Utility Companies

Modelo genérico para el envío de alertas seguras en empresas del sector energético

Galván-Bobadilla I.
Instituto de Investigaciones Eléctricas.
Cuernavaca, Morelos, México.
E-mail: igalvan@iie.org.mx

Santos-Domínguez M.
Instituto de Investigaciones Eléctricas.
Cuernavaca, Morelos, México.
E-mail: msantos@iie.org.mx

Perez-Díaz J.A.
Tecnológico de Monterrey, Campus Cuernavaca.
Cuernavaca, Morelos, México.
E-mail: jesus.arturo.perez@itesm.mx

(Recibido: abril de 2008; reevaluado: enero de 2009; aceptado: febrero de 2009)

Abstract

In some industries such as logistics services, bank services, and others, the use of automated systems that deliver critical business information anytime and anywhere play an important role in the decision making process. This paper introduces a "Generic model to send secure alerts and notifications", which operates as a middleware between enterprise data sources and its mobile users. This model uses Short Message Service (SMS) as its main mobile messaging technology, however is open to use new types of messaging technologies. Our model is interoperable with existing information systems, it can store any kind of information about alerts or notifications at different levels of granularity, it offers different types of notifications (as an alert when critical business problems occur, as a notification in a periodical basis or as 2 way query). Notification rules can be customized by final users according to their preferences. The model provides a security framework in the cases where information requires confidentiality, it is extensible to existing and new messaging technologies (like e-mail, MMS, etc). It is a platform, mobile operator and hardware independent. Currently, our solution is being used at the Comisión Federal de Electricidad (Mexico's utility company) to deliver secure alerts related to critical events registered in the main power generation plants of our country.

Keywords: Mobile middle ware, mobile environments, nomadic computing.

Resumen

En algunas industrias como las empresas de generación eléctrica, consultoras de servicios de logística, banca y otras, el uso de sistemas automatizados que entreguen -en cualquier

lugar y en cualquier momento- información crítica del negocio, juegan un papel muy importante en el proceso de toma de decisiones. En este artículo se presenta un "modelo genérico para enviar notificaciones y alertas en forma segura", el cual opera como una capa intermedia entre las fuentes de datos empresariales y sus usuarios móviles. Este modelo usa el servicio de mensajes cortos o Short Message Service (SMS) como su principal tecnología de mensajería, no obstante, está abierto a usar nuevas tecnologías de mensajería. Nuestro modelo es interoperable con sistemas informáticos existentes, es capaz de almacenar en distintos niveles de granularidad cualquier tipo de información sobre alertas o notificaciones, ofrece distintos tipos de notificación (por ejemplo: como alerta cuando ocurre algún problema crítico del negocio, como una notificación en forma periódica ó como una consulta de dos vías). Las reglas de notificación pueden ser personalizadas por los usuarios finales, de acuerdo a sus preferencias. El modelo ofrece un marco de seguridad para aquellos casos en que la información requiere ser protegida, además es extensible con nuevas tecnologías de mensajería. Es independiente de hardware, sistema operativo y operadora de telefonía celular. Actualmente, nuestra solución se encuentra en uso por la Comisión Federal de Electricidad para enviar alertas seguras relacionadas con eventos críticos ocurridos en las principales plantas de generación eléctrica de nuestro país.

Descriptores: *capas intermedias móviles, ambientes móviles, cómputo móvil.*

Introduction

Medium to large size organizations have a variety of information systems like administrative, operative or strategic applications; these applications contain very valuable and helpful information for the decision-making process. Usually, these systems need to be consulted from a desktop computer so the user can be informed of critical information.

There are scenarios where users have no access to a desktop computer because most of their time is spent in continuous movement outside of their offices, and some of these users are persons who are responsible for taking critical decisions for the company. This group of users requires mobility and ubiquitous access to information at the moment that is needed.

Hence, there is a need to have a tool that monitors and unifies critical business information which delivers it to decision makers as quickly as possible in pocket-sized devices, in a secure way, anytime-anywhere and also eliminate the need for wires.

An alternative to solve those necessities is the creation of a "middleware" between data sources and final users that make use of mobile messaging as an instantaneous medium of communication.

Such middleware must resolve the following challenges (see figure 1):

A) *Interoperability with existing systems*. Usually, data sources are heterogeneous; information is stored in different database management systems and acceded through applications created in distinct programming languages.
The middleware must provide a standard mechanism for connecting to data sources without concerning the technical aspects where they were created.

B) *Handle different kinds of notification contents*. Notification data in a certain domain may not be the same in another domain, so a flexible repository design must be considered to store any kind of information related to a notification service.

C) Confidentiality and integrity of messages have to be assured, especially when classified data is transmitted.

D) *Different mobile messaging technologies and devices to notify*. The content of messages needs to be transformed to a proper format according to the type of device where the message is going to be read.

E) *Users require customizing their notification preferences*. There are some cases where alerting services are too general, and users need to customize their notification preferences according to their information needs.
For example: if the alerting system consists of notifying the presence of hurricanes, maybe a user who is living in the west will decide to only receive alerts of hurricanes from the Pacific Ocean.

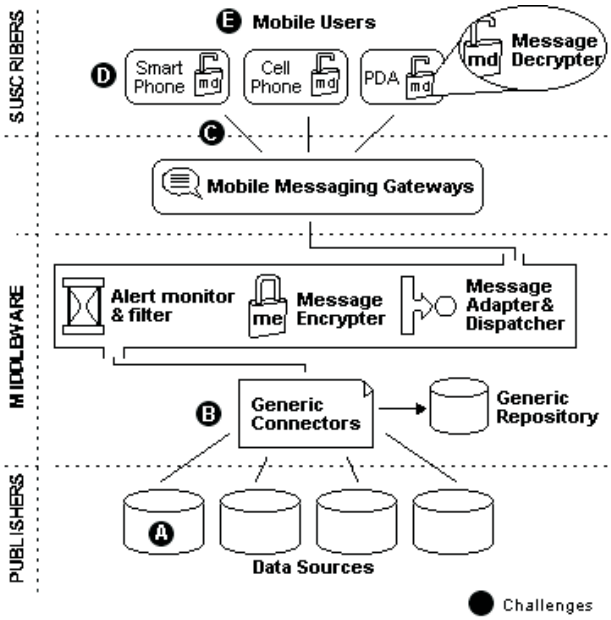

Figure 1. Architecture and Challenges of the Proposed Solution.

Selected technologies and related work

As part of this research, we made an analysis of the current Mobile Messaging Technologies (MMT) in order to decide which of them is more suitable to our country.

Currently there are three MMTs: *Short Message Service* (SMS) (2002), *Enhanced Message Service* (EMS) and *Multimedia Messaging Service* (MMS). Table 1 summarizes all the features of each technology.

Table 1. Main Features of Mobile Messaging

SMS	- Sends text plain-based messages with a length up to 160 characters, although concatenation of messages is allowed. - Offers a "Store and forward" service for traffic management, delivers the message when the user turns on his mobile equipment. - Cheap, also offers international roaming without charges. Is included in all cell phones, from the most basic to the most sophisticated.
EMS	- Emerged as an upgrade for SMS. - Allows sending formatted text, grayscale images and melodies. - Is a 3GPP Standard. - Is not supported in all cell phones. - Its price varies depending on the content of the message. Not commonly used, surpassed by MMS.
MMS	- The most modern system for mobile messaging - Allows the user to send: formatted text, graphics, data, animations, voice transmissions, video and audio clips - It is based in SMIL (also based in XML) to customize the flow of displaying multimedia elements. Expensive costs per message, also requires sophisticated and costly equipment.

SMS is the most used technology in the world. According to Garnet Dataquest Group, one of the industry's major research agencies, it is estimated that in 2002, 142 billion SMS messages were exchanged worldwide, and 168 billion in 2003 (Le Bodic, 2003). In México the use of SMS is intensive; from 2003 to 2005 SMS increased by 500% (Olguín, 2006). On the other hand, its cost is very low: 85 cents of a peso, compared with MMS that costs 13 pesos per message (The net size guide 2006) plus download charges.

The previous information motivated this work to focus on the use of SMS as a default technology to send alerts, in addition to the following: it is very cheap; it is available in many countries; it is present in any cell phone; it is interoperable between different cell phone companies; offers "store and forward messaging", that means, that when a user has "turned off" his mobile, the SMS center holds the message until the user turns "on" his equipment; and many other advantages mentioned in Drumea *et al*. (2004) and Ravi *et al*. (2004).

Related work

Before starting with the design of our proposed model, we made an analysis of previously related work on the use of mobile messaging for sending alerts (see table 2).

We found the following disadvantages: they are expensive tools; they are proprietary and domain specific; they do not offer security on the transmission of messages; they are operating system dependant and are limited to a specific mobile technology; and they do not allow the customization of notification preferences.

The work described in (Wams *et al*., 2003) is an abstract model that it is implementation independent, so features G, H, I and J are not available. On the other hand, security is achieved by using hybrid protocol based on public and private keys; however this requires bigger processing requirements that are not suitable for many mobile devices. Ravi (2004) offers very poor security: data is only encoded (not encrypted); access rights are based on a plain user-id.

Table 2. Available Tools for Sending Alerts Using Mobile Messaging

Tools	Admin. tools			Notification Models			Technological advantages				
	A	B	C	D	E	F	G	H	I	J	K
[6]	Y	N	N	N	Y	N	N	*	*	N	N
[7]	Y	N	Y	N	Y	N	N	N	Y	N	N
[8]	Y	N	N	N	N	N	N	N	Y	Y	N
[9]	Y	N	Y	S	Y	Y	N	N	Y	Y	N
[10]	N	N	N	N	Y	Y	N	N	Y	Y	N
[11]	N	P	Y	Y	Y	N	Y	Y	Y	Y	N
[12]	N	N	Y	Y	Y	N	*	*	*	*	P
[13]	N	N	Y	Y	N	N	N	N	Y	Y	P
[14]	N	N	N	N	Y	N	N	N	N	Y	N

Y = Yes, N = No , P = Partially, * = Not available

A	Subscribers groups management	G	Extensible to new messaging technology
B	Customize notification preferences	H	Multiplatform
C	Interoperability with existing systems	I	Hardware Independent
D	Periodical	J	Operator independent
E	Per event	K	Security on transmitted msg
F	2 Ways support		Opportunity areas

SMS Based Generic Model
To send secure notifications in real time systems

After analyzing the previous work, we concluded that it was necessary to create a cheaper solution that eliminates all the disadvantages that the other tools have. Figure 1 shows the architecture of the proposed model.

Generic connectors

In order to be able to communicate the middleware with any data source (challenge A), we created a couple of documents (called generic connectors) based on XML [1]; the advantage of using XML is that publishers just need to generate (or "push") two outputs based in our proposed XML structure.

The first output (called XMLAlertDef) is generated only once and is used by the publishers to describe what the alert consists of (See figure 2).

A tipical *XMLAlertDef* document will include: the alert's name, the alert's description, who is the publisher, how often information will be published, if it has support for two-way messaging and (optionally) the name and type of additional information that can be included as "extra_parameters" in the content of an alert's message.

The second output (called XMLAlertData), is used by publishers to issue the message content of an alert, this document is generated when new information is registered at data sources (See figure 3).

The use of "extra_parameter" tags are very useful when the publisher wants to add more data granularity to the alerting service, for example, if the alerting service is Temperature of Mexico City the "extra_parameters" tags will probably include data like: humidity, UV Index, precipitation probability, etc. In the other hand, the subscriber can take advantage of the information contained in the "extra_parameter" tags to customize his notification preferences based on its contents.

The "extra_parameters" are also used to solve any kind of information related to a notification service (challenge B).

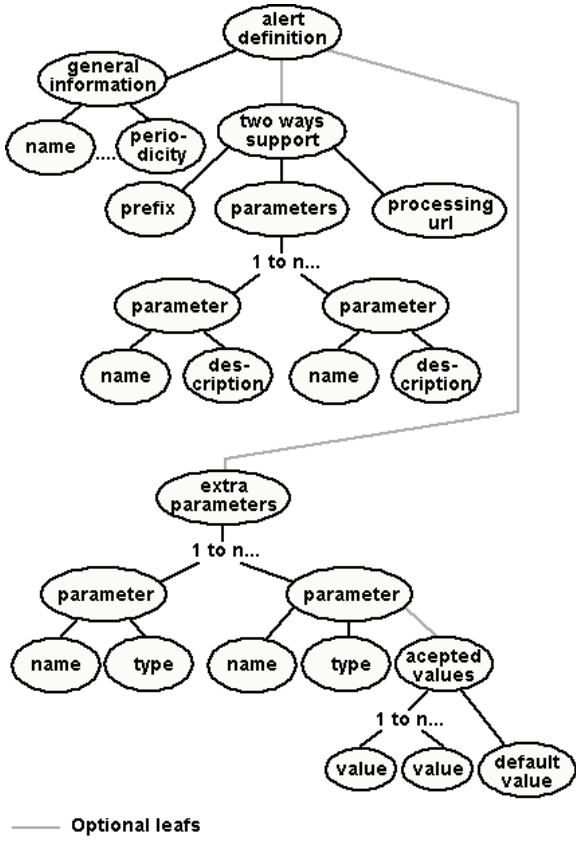

Figure. 2. XMLAlertDef Document Estructure

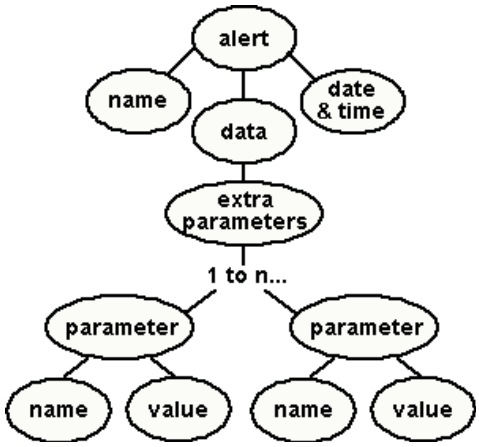

Fig. 3. XMLAlertData Document Estructure

Alert's monitor

This component works in three modes: per event mode, "two ways" mode and periodical mode.

Per event mode:

There are some scenarios where information is generated in a random, unpredictable or unexpected way, for example, an earthquake, a fault in a power station, the increase or decrement of auctions, etc. On this type of scenarios, the "per event" monitoring mode is used.

Similar to the "event streams" described in Chen (2002), in the per event mode, publishers have the responsibility to identify and deliver new information. It is more efficient that the publisher "push" information when generated instead of having a monitor checking continuously data sources and consequently consuming resources such as bandwidth, DB connections, processor time, etc.

The monitor is "listening" for new data and when this occurs it verifies the authenticity of the data source and if it is valid, proceeds to create a list of subscribers for that alerting service. Later, for each subscriber, it carries out a process called "parameters collation" (explained in section 4.3) to verify if the received data "matches" with the user's notification preferences. In the case of a match, it checks on which mobile equipment and MMT the notification must be sent.

Finally, based on that information, the middleware adapts and dispatches the message using the appropriate Mobile Messaging Gateway (MMG). A MMG is a hardware and software component that serves as an access point to other networks; it makes the conversion of protocols between different types of networks or applications. Figure 4 shows the flow diagram for this mode.

"Two ways" mode:

In this mode, the way that information travels is different; in this case the mobile user sends a request using a message (See figure 5). This message includes a prefix, 2-ways parameters and the source's equipment ID. The "prefix" parameter is used by the monitor to identify the alerting service which will process the request, the 2-way parameters are optional and they are used by the data source system as a filter of information, finally the equipment ID is later used by the MMG to return to the subscriber the results of the query.

Periodical mode:

This monitoring mode is used when information at data sources is generated on a regular basis, so the middleware knows how often new information will be available. Examples of this type of information are the amount of sales in a week, the daily price of fuel and other raw materials, the monthly complaint summary, etc.

This mode is similar to per event mode, the only difference is that the monitor is continuously consulting data sources (based on the notification period specified by the publisher).

The minimal time for monitoring is every hour and the maximum is every year. When new information is discovered, a similar process like "per event mode" is carried out.

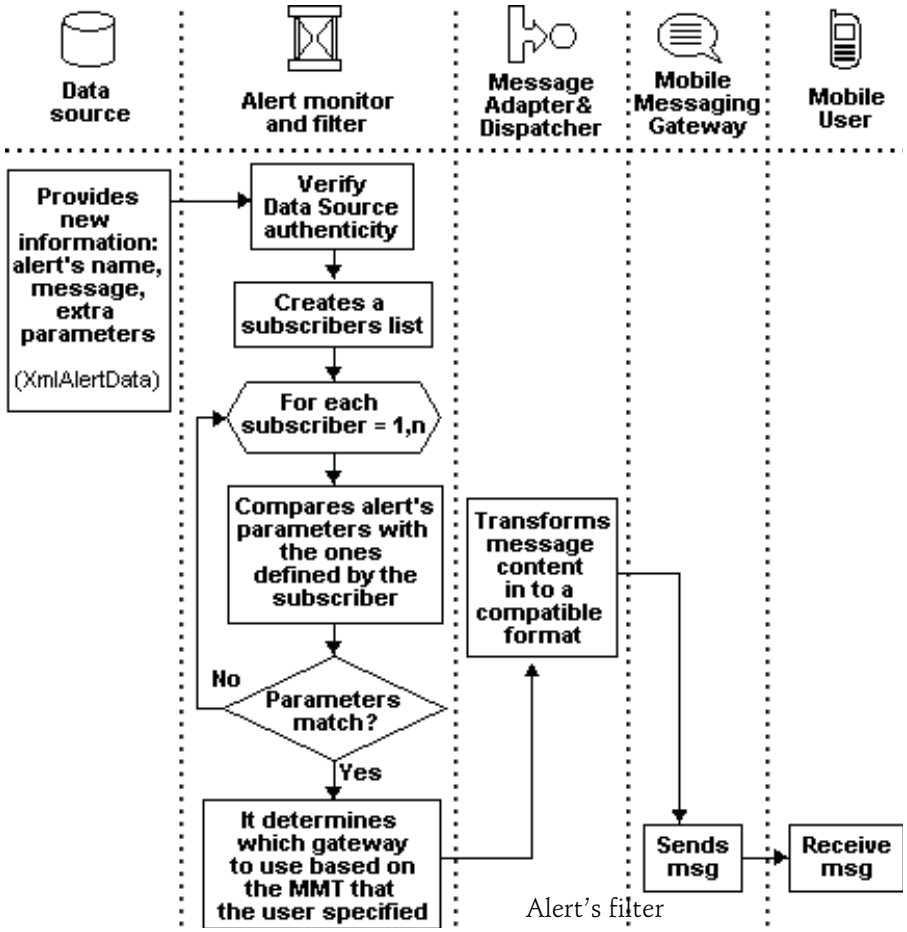

Figure 4. "Per Event" monitoring mode

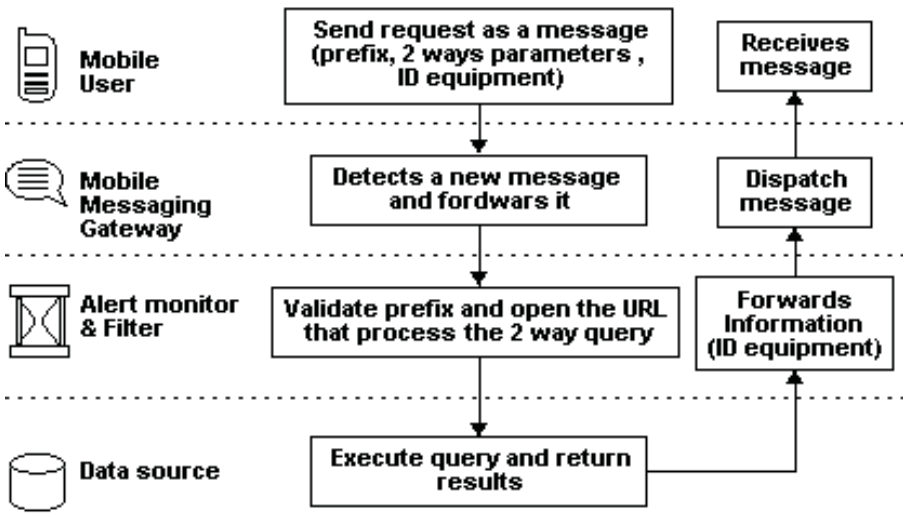

Figure 5. "Two ways" monitoring mode

With this component, the middleware determines if an alert must be sent to a subscriber or not. This is achieved by doing a Parameters Collation Process (PCP). See figure 6.

The PCP analyzes and compares each "extra_parameter" tag included in the XMLAlertData Document against the parameters that were customized by the subscriber. In the case that all the "extra_parameter" values satisfy the conditions indicated by the subscriber, the alert must be sent. On the contrary, the alert should be ignored.

Figure 6 shows an example of the PCP, in that example, Subscriber A is the only one who is going to receive an alert because all his conditions are satisfied.

The PCP is a novel feature that allows subscribers to customize their notification preferences when no alert's history is stored in the middleware's database. The PCP was not found in any of the related work (challenge E).

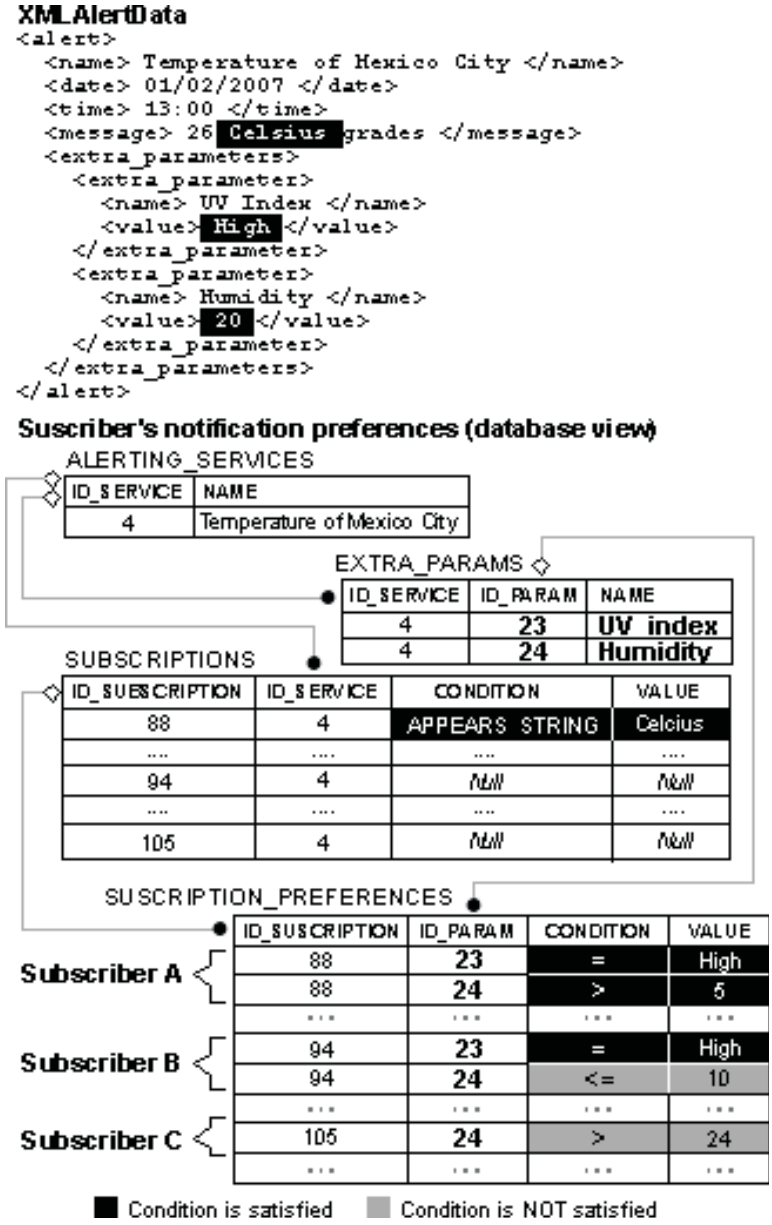

Figure 6. Example of the Parameter Collation Process (PCP)

Our middleware also offers templates that include common notification preferences, with this feature a subscriber can save time at the customization of notificacion preferences process. In future work, our middleware will include Artificial Intelligent techniques to decide when an alert should be sent based on the alerts sent to subscribers in the past.

Message adapter and dispatcher

Based on Haneef *et al*. (2004) we developed a Message Adapter (MA) component, that transforms the content of a message in to a proper format in order to suite the capabilities of the target device, for example, if the subscriber wishes to receive an alert via MMS the MA transforms the content of the alert (the XMLAlertData Document) into SMIL [3]. SMIL is the used language for creating MMS messages. If another subscriber wants to receive an alert as an e-mail then the MA transforms the message into HTML, etc. The MA uses XSLT [4] as its core technology (see figure 7).

With XSLT the rules about how the middleware has to transform an alert into specific format are provided as external instructions that can be updated or removed without affecting the middleware's operation. If a new MMT is created and the middleware wants to use it, the middleware's administrator only needs to register the new MMT and attach its corresponding XSLT document.

By using a MA the middleware is extensible to other messaging technologies (so challenge D in figure 1 and feature G in table 2 is achieved).

The MA is a feature that was not found in any of the previous work. We succesfully tested our MA transforming XMLAlertData to SMS, HTML and email. Future work will include voiceXML, SMIL and SVG transformations.

Message encrypter & decrypter

As we mentioned in section 2, we focused on the use of SMS as a default MMT. However, SMS does not consider any security features, hence, information is transmitted as plain text, and therefore, it is susceptible to malicious attacks like eavesdropping and data alteration (Talukder, 2003).

This is a problem when the type of information to be transmitted is classified. To avoid these problems we propose a Message Encrypter (ME) in the middleware and a Message Decrypter (MD) at the end user's mobile equipment, as illustrated in figure 1.

The message Encrypter seeks (inside of the middleware database) the subscriber's password and uses it as a symmetric key to encrypt the message to be sent. The subscriber's password was previously provided when the user subscribed to an alerting service. Figure 8 shows the message protection process.

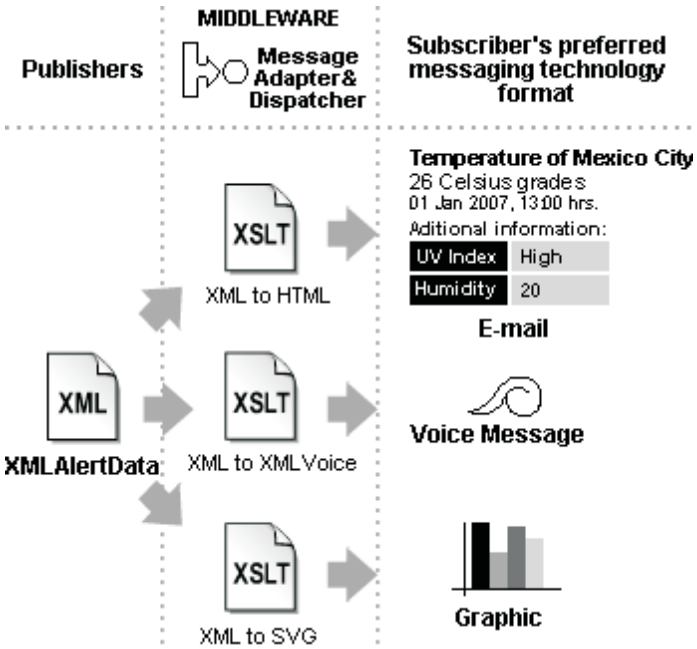

Figure 7. Examples of Different Formats Generated by the MA

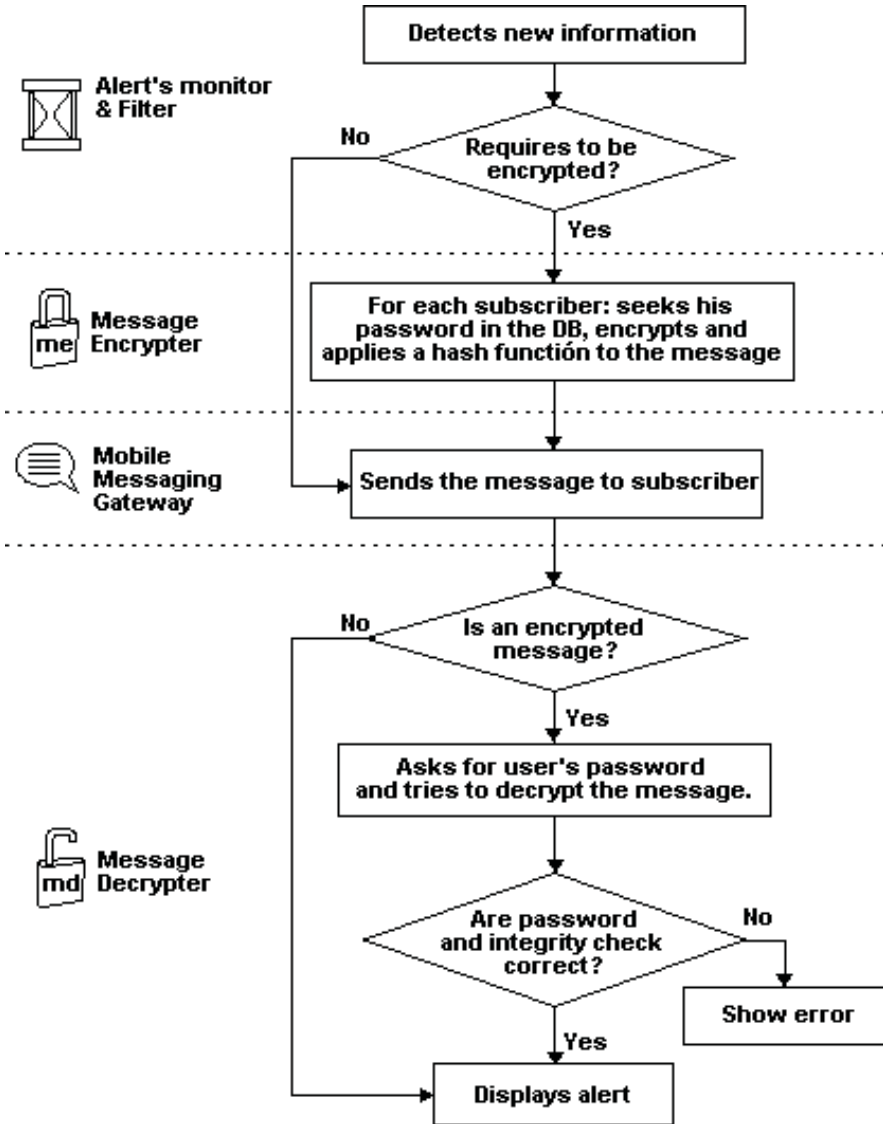

Figure 8. Message Protection Process

The use of an encrypter and decrypter component is a feature was not found in any of the related work and that is used to assure the confidentiality of SMS (challenge C). Authentication is out of the scope of our middleware, because this is done when the subscribers registers his mobile equipment to the notification service. We assume that additional authentication is made by the mobile carrier when the subscriber's mobile is connected to the network.

With the encrypter and decrypter components, our model is a cheap and safe solution that can be used to deliver confidential SMS in several domains where information is classified, for example, to send a password to activate a system, a credit card number for bank transactions, the name and diagnosis results of a patient in a hospital, the amount of sales of a store, the geographic coordinates of an important shipment, etc.

Implementation

The proposed model was implemented and distributed in several hardware and software components. Currently, it is being successfully used in a real world application at the Comisión Federal de Electricidad (CFE) (2007) to deliver secure alerts related to critical events registered in the main power generation

plants of our country. CFE is the utility company in Mexico. Figure 9 shows the distribution diagram of the implemented model. However, a smaller hardware and software distribution can be made to reduce costs which would be easy to install in small businesses.

The alert monitor and filter, the message encrypter and the message adapter and dispatcher were implemented as a Java 2 SE desktop application, which operates as thread that is continuously executed to search new alerts.

Another important part of our implementation is mAlert, which is a web application where the middleware's administrator can register and manage alerting services, supported devices, MMTs, MMGs and subscribers. Additionally, mAlert provides a public area where mobile users can subscribe to alerting services and customize their notification preferences (see figure 10).

Concerning the confidentiality and integrity of SMS, the Message Encrypter and the Message Decrypter was implemented using symmetric cryptography based on AES (Daemen, *et al*., 2002) and SHA-2 (Eastlake *et al*., 2006). We selected AES algorithm because it is the best and current encryption standard, and there is a current implementation available. A stronger cryptosystem is not required because the alert's data is not considered to be top secret stuff.

Message Decrypter was specifically implemented as a mobile application (MIDlet) based on J2ME [2] / MIDP2.0 (2002) that can be executed in a PDA or a Cell Phone, this application is listening for incoming ciphered SMS at a specific port number.

When a new secure SMS arrives at the mobile device the application is launched and asks the user for a valid password in order to display the message, as illustrated in figure 11.

In order to send secure SMS to a specific port number in a mobile device, we developed our own SMS gateway (called *mGateway*). *mGateway* is a multiplatform application (created in Java) that is capable to manipulate (Through AT Commands, 2003 in PDU mode) any cell phone or GSM MODEM (based on ETSI standard) connected by a COM port to send SMS. *mGateway* includes inside of the SMS message information about: the port number where the message has to be sent (port addressing), the size of the message, the payload, the digest and other extra parameters, as illustrated in figure 12.

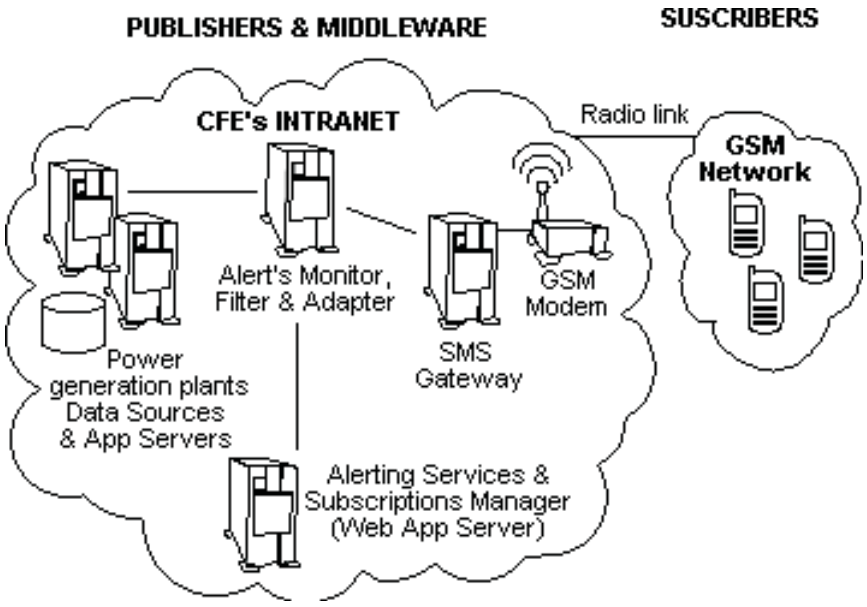

Figure 9. Distribution diagram for medium and large size companies

Figure 10. Web interface for customizing notification preferences

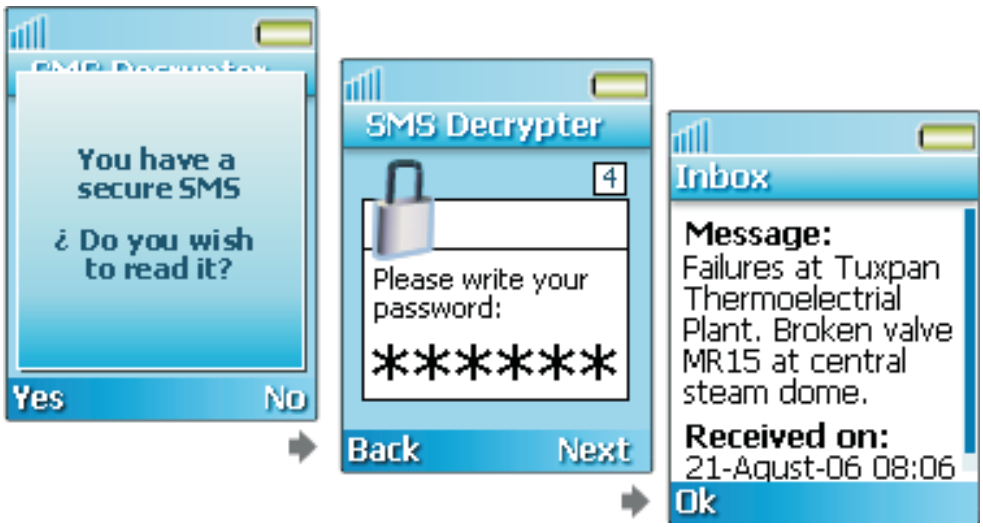

Figure 11. Message Decrypter main user interfaces

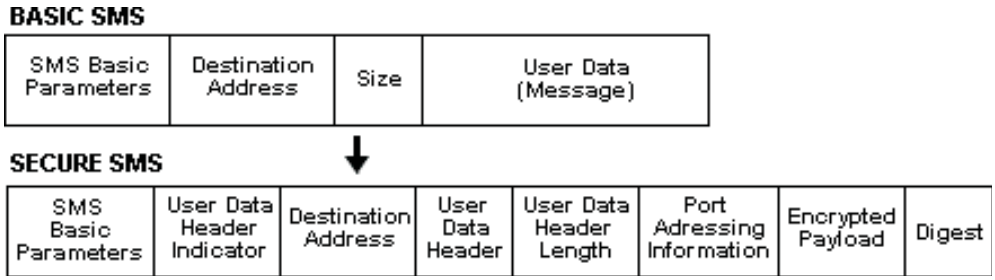

Figure 12. Secure SMS format created by mGatetway

Potential aplications

Although our current implementation is being used by the utility sector, our model can be extrapolated to other domains like banking services, logistic and financial services. The following is a list of examples where the proposed model can be used:

1. Alerts about unsafe operation levels in production plants.
2. Notifications about fuel price variations.
3. Earthquake and infrastructure impacts reports.
4. High traffic warnings.
5. Bad weather and disaster alerts.
6. Notification of expired payments.
7. Notification of important banking transactions.
8. Notification of daily revenues in small business.
9. Low stock warnings.

Future work

During the testing of our work we identified that performance and wait times presented a variation between different mobile devices, network technologies and network providers.

Future work will implement a similar model like the one is exposed in Wittie *et al*. (2007), in order to manage a fine tunning to our application code to ensure consisten behavior across platform types and network providers, and by consequence to assure a good aplicaction usability and performance.

Conclusions

There are many areas where the benefits of mobile messaging can be exploited. The proposed model provides an easy and fast way to implement it.

Our current implementation has contributed to the decision making process of the CFE's power generation area. It is being successfully used at 300 thermoelectric power plants where supervisors can be well informed about failures and anomalies in the production process. In the near future, the CFE will use our implementation to provide alerting services about unsafe water levels in dams at hydro power plants.

The use of XML as a universal connector for publishing alerts facilitates the integration of existing information systems with the proposed middleware.

The use of "extra_parameters" tags allows storing any kind of information about an alert and helps to provide a depth level of granularity in the contents of an alert.

The Parameter Collation Process (PCP) takes advantage of the existence of the "extra_parameters" tags in order to allow subscribers to customize their notification preferences. Both PCP and "extra_parameters" are useful and novel features that were not found in any of the related work.

The use of XSLT converts our model to an extensible tool to new mobile messaging technologies. The integration of encryption mechanism and the use of SHA-1 contribute to the area of security of SMS, which was not considered by its creators.

The creation of a Java based mobile messaging gateway capable of connecting to GSM modems via serial communication offers great flexibility to companies that need to incorporate SMS based services at a lower cost, because they do not require expensive hardware, a specific cell phone carrier, and a specific operating system.

Acknowledgments

This research was supported by research grants from the Mexican Electric Research Institute (IIE).

References

AT Command Set for User Equipment (UE) 3GPP TS 27.007 V3.13.0 (2003-03). 3rd Generation Partnership Project.

Bulk SMS India–NonStopSMS.com–India's First Website Dedicated to Bulk SMS solutions [on line]. [January 10, 2006]. Available on: http://www.nonstopsms.com.

Comisión Federal de Electricidad (CFE). Mexico's Utility Company [on line]. [Januar, 2007]. Available on: http://www.cfe.gob.mx/en.

Daemen J., Rijmen V. *The Design of Rijndael: AES-The Advanced Encryption Standard*. Springer-Verlag. 2002. ISBN: 3540425802.

Dantas M.A.R., Baggio R.K. A SMS Tool for Alerts and Monitoring of a High Availability Cluster Environment. IEEE 19th International Symposium on High Performance Computing Systems and Applications, 2005, pp. 307-11. ISBN: 0 7695 2343 9. 15-18 May 2005, Guelph, ON, Canada.

Drumea A., Svasta P., Popescu C. Remote Access Solutions for Industrial Control Systems. 27th International Spring Seminar on Electronics Technology: Meeting the Challenges of Electronics Technology Progress, Vol.1, Pages 30-35. IEEE, Institute of Electrical Engineers. 13-16 May 2004.

Eastlake D., Hansen T. US Secure Hash Algorithms (SHA and HMAC-SHA), RFC 4634 [on line]. [July 2006]. Available on: http://tools.ietf.org/html/rfc4634

Chen G., Kotz D. Solar: An Open Platform for Context-Aware Mobile Applications. In Proceedings of the First International Conference on Pervasive Computing, pp. 41-47, June, 2002.

Haneef A., Ganz A. ANMoLe–An Adaptive Multimedia Content Delivery Middleware Architecture for Heterogeneous Mobile Multi-Device Neighborhoods. *International Journal of Multimedia Tools and Applications* (Kluwer Academic Publishers), 22(2):171-186, February 2004.

Jain R., Puglia S., Wullert J., Parmeswaran K., Bakker J. The Mobile Application Server (MAS): An Infrastructure Platform for Mobile Wireless Services. *Information Systems Frontiers*, 6(1):23-34. Mar. 2004. ISSN: 1387-3326. Springer Netherlands.

Le Bodic G. *Mobile Messaging Technologies and Services: SMS, EMS and MMS*. John Willey & Sons. 2003. P. 36. ISBN: 0-470-84876-6

Message Master™ Enterprise Alert, SMS Software for Enterprises. Derdack GmbH. Germany [on line]. [February 15, 2006]. Available on: http://www.derdack.com/products/EA.htm.

Mobile Information Device Profile 2.0 Java Community [on line]. [2002]. Available on: http://jcp.org/aboutJava/communityproess/final/jsr118/index.html

Olguín-Sánchez J. Quintuplican envío de mensajes cortos [on line]. Pagina oficial de la Presidencia de la República [January 10, 2006]. Available on: http://www.presidencia.gob.mx/buscador/index.php?conteido=17470&pagina=1&palabras=sms.

Ravi S., Chathish M.S., Prasanna H. WAP and SMS Based Emerging Techniques for Remote Monitoring and Control of a Process Plant. On: 7th International Conference on Signal Processing Proceedings (ICSP'04), 2004, p. 2672-2675. ISBN: 0-7803-8406-7. IEEE, Institute of Electrical Engineers. Aug 31-Sep 4 2004, Beijing, China.

Small Screens a Global Vision, The Net Size Guide. Net Size S.A. Paris France. February 2006. ISBN: 2 -9523533-1-X

SMS Messaging Software From NotePage. NotePage Pro [on line]. [January 12, 2006]. Available on: http://www.notepage.net/.

Talukder-Asoke K. Information Assurance and Security needs in an ASP/MVNO Environment for Pervasive Content through SMS/GSM. International Conference on Communication and Broadband Networks. May 5-7, 2003. Bangalore, India.

Technical Realization of the Short Message Service (SMS), Release 1998, 3GPP TS 03.40 V7.5.0 (2001-12). 3rd Generation Partnership Project (3GPP). France, 2002.

Telcel–DATUM. SMS Alerts Generated by Systems Logs [on line]. [January 10]. Available on: 2006http://www.datumtelcel.com/fr_contenidos.html?op=01.

What is NowSMS? [on line]. [February, 2006]. Available on: NowSMS.com. http://www.nowsms.com/whatisnowsms.htm.

Wams J., Van Steen M. A Flexible Middleware Layer for User-to-User Messaging. In Proc. 14th International Conference on Distributed Applications and Interoperable Systems, Lecture Notes on Computer Science, Nov. 2003. Springer-Verlag, Berlin.

Wittie M.P., Stone-Gross K.C. Almeroth and Elizabeth M. Belding.MIST: Cellular Data Network Measurement for Mobile Applications. Proceedings of IEEE Broadnets, Raleigh, NC. September 2007.

[1] [Extensible Markup Language (XML). World Wide Web Consortium (W3C) [on line]. Available on: http://www.w3.org/XML/.

[2] [Java ME-Micro App Development Made Easy. Java Technology [on line]. Available on: [http://java.sun.com/javame/index.jsp

[3] [SMIL, The Synchronized Multimedia Integration Language. World Wide Web Consortium (W3C) [on line]. Available on: http://www.w3.org/AudioVideo/

[4] [XSL Transformations (XSLT). World Wide Web Consortium (W3C) [on line].Available on: http://www.w3.org/TR/xslt

About the authors

Israel Galván-Bobadilla. Received the B.S. degree in computer systems from Universidad de Occidente, Campus Guasave, Sinaloa, Mexico, in 2000 and the Masters degree in Computer Science from the Tecnológico de Monterrey, Mexico, in 2006. Since 2001, he has been with the Electrical Research Institute, Cuernavaca, Morelos, Mexico, where he has developed several information systems for the Mexican power sector.

Martín Santos-Domínguez. Received the B.S. degree in Physics from Universidad de Veracuz, Mexico, in 1987 and the M.S. degree in fiber optics from the University of Salford, England, in 1994. He has experience in the development of virtual instrumentation systems and image processing, LAN/WAN networks design, installation and management; he also has worked in the multimedia applications field with the use of integrated audio and video services. Since 1998, he has been with the Department of Information Systems at the Electric Research Institute, Mexico, where he is a Project leader. He has directed numerous information system projects for the Mexican Petroleum Company and the CFE (the main utility company of Mexico).

Jesus Arturo Pérez-Díaz. Obtained his B.Sc. degree in Computer Science from the Universidad Autonoma de Aguascalientes, Mexico, in 1995. He worked as a system and network administrator in the Aguascalientes city hall. He got his PhD Degree in Computer Science in the University of Oviedo in 2000. During his PhD studies, he carried out research in mobile agents and published around 12 research papers in magazines and international conferences and became a full associate member of the European founded research project AgentLink. Nowadays he is a researcher and professor in the Tecnologico de Monterrey, Campus Cuernavaca and member of the Mexican Researchers National System, his research field focus in network security and wireless communications. Currently Jesús Arturo Pérez-Díaz holds the recognized Cisco certifications CCNA and CCAI, which allows him to give Cisco certification courses. He has given security courses in some European and South American Universities.