VESMP (VERY SHORT MESSAGE PROTOCOL) AN SMS-BASED PROTOCOL FOR PROCESS MONITORING AND SYSTEM REMOTE ADMINISTRATION

Thomas Ndie Djotio, Claude Tangha
Department of Computer Science, LABORIMA, Ecole Nationale Supérieure Polytechnique de Yaoundé
University of Yaounde I, PoBox 8390 Melen, Yaounde, Cameroon

Georges Edouard Kouamou
Department of Computer Science, LABORIMA, Ecole Nationale Supérieure Polytechnique de Yaoundé
University of Yaounde I, PoBox 8390 Melen, Yaounde, Cameroon

Keywords: Protocol, process monitoring, remote administration, Short Message Service (SMS).

Abstract: In this paper we propose a Very Short Message protocol (VeSMp), a simple SMS-based protocol for process monitoring and system remote administration. This protocol offers the system administrator an additional means of supervising and monitoring the activity or the state of processes and services via a mobile terminal. VeSMp transforms a Global Mobile Standard (GSM) terminal by means of SMS service into a true station of system administration as well as a PC connected to a corporate network. This protocol uses an original concept which we call VeSM (for Very Short Message). VeSM represents a very short message, an alias or extensible shortcut which makes it possible to implicitly exceed the conventional limit of 160 characters maximum used in SMS.

1 INTRODUCTION

This paper presents the integration of Short Message Service (SMS) technology in the process of system administration in general, and in the field of process monitoring in particular. Indeed, the SMS became very popular in Europe and Asia where more advanced numerical networks made it available long before it started in North America (Pons, 2001). It is less than one decade since Global Standard for Mobile (GSM) technology was popularized in the developing countries including Cameroon. New applications of this service are increasing each day (Enck et al., 2005), (Trosby, 2004), (NewNet SMserverTM, 1999), (Wikipedia, 2006). For the owners of GSM terminals, it is an alternative to lower costs in terms of communication. For certain economic operators, it is an added value of service (Ngadeu, 2003) making it possible to improve the profitability of the company as well as a traditional product on sale in the case of hardware shops. For us it is an opportunity of offering a system administrator an additional means to improve activities of system monitoring in companies and especially in Small and Medium-sized Businesses (SMB), where the presence of a System administrator is not basically essential in permanence.

In terms of system and network monitoring, the company faces the following problems today: necessity to manage the availability and the performances of new applications and network services, increase in the number of mobile personnel; and security. In response, we propose solutions based on technologies of lower cost to carry out the tasks and large scale actions. These solutions at average scale have impact on the development and the blooming of SMB.

We propose the VeSMp protocol, an original alternative of exploiting the SMS service for remote administration and the monitoring of processes. The idea, born from a simple report is motivated by the growing interest that mobile users of telephones and the companies attach to SMS technology. We also introduce here an original concept called VeSM

Ndie Djotio T., Tangha C. and Edouard Kouamou G. (2007).
VESMP (VERY SHORT MESSAGE PROTOCOL) AN SMS-BASED PROTOCOL FOR PROCESS MONITORING AND SYSTEM REMOTE ADMINISTRATION.
In *Proceedings of the Second International Conference on Wireless Information Networks and Systems*, pages 25-32
DOI: 10.5220/0002144600250032

which allows for circumventing the conventional limit of the maximum number of characters which an SMS can contain. Our approach in this article first uses a state of the art which extends the fundamental concepts related to the principles and operations of SMS service, system monitoring and the logic of establishing a protocol of management. Secondly, we present the description of VeSMp, our protocol of communication. It consists of presenting its model and architecture, and also the abstractions which made it possible for its realisation. We end up by showing how VeSMp is integrated into the standards of network management like Simple Network Management Protocol (SNMP) of Transport Control Protocol/Internet Protocol (TCP/IP) and Common Management Information Protocol (CMIP) of Open System Interconnection (OSI) (Pugolles pp 829-876, 2002).

2 STATE OF THE ART

Compared to the Internet which is seen today as the greatest technological revolution of the century, the success of SMS service has taken their providers by surprise, the operators of GSM (Trosby, 2004).

2.1 Short Message Service (SMS)

The SMS offered by the GSM network appeared on the scene for the first time in 1991 in Europe and is defined as "a globally accepted wireless mobile service that enables the transmission of alphanumeric messages between mobile subscribers and external systems such as electronic mail, paging and voice mail systems" (NewNet SMserverTM, 1999). However, it is since the 1980s that experts in the communities of GSM operators thought of additional services based on text messages in their offers in addition to those already existing, such as voice in particular (Wikipedia, 2006).

This service of text messages of a maximum length of 160 characters (coded using ASCII 7 bits on 140 bytes) makes it possible for a user to carry out, starting from his mobile terminal, the transfer of messages to one or more recipients having GSM mobile telephones equally or to a similar external entity with GSM network called Shorts Message Entity (SME) (Pons, 2001). The exchanges of short messages (textos or SMS by abuse) are possible thanks to the network of Signaling System n°7 (SS7) (Trosby, 2004), (Pons, 2001). Given the differences with other existing text services like paging, SMS service guarantees the delivery of messages by the network (NewNet SMserverTM, 1999), while temporary failures are identified and short messages are stored on the network until the recipient becomes available. Indeed, if the latter is available, the message is directly transmitted to him on his terminal, if not; it is stored on a central server of short messages SMS Center (SMSC) through which it passes. The SMSC ensures the storage of the Short Message (SM) in databases like Gammu (gammu.org, 2006). Gammu is a project which encompasses applications, scripts and drivers for managing various functions on cellular phones and similar devices. It also ensures the distribution of SM to mobile terminal recipients (when these appear in the GSM network to which they belong) in the limit of their date of validity. The logical channels of voice and data transmission are separated so that the two services can simultaneously be available. As soon as the mobile terminal is identified, the network informs the SMSC that it can successfully deliver the message to its recipient. The SMSC is located by a telephone number pertaining to the Public Mobile Land Network (PLMN). The dialogue between the SMSC and the mobile terminal is done through the Mobile-services Switching Center (MSC) (Pons, 2001).

The missions initially assigned to the SMS service are today largely exceeded. There are many examples of operating the SMS service. Today several Internet services are coupled with SMS. They include: email, instant messaging, the services of information (climatology, meteorology), interactive banking, etc. The benefits of SMS are today very numerous (Wikipedia, 2006), (Girondo Stéphane), (De Wulf, 2001). Authors in reference (NewNet SMserverTM, 1999) propose an inexhaustive range of the most outstanding SMS services today. We mention some here:

- Reminder/calendar to point out appointments, meetings or important events.
- The reservation of places on trains, planes or other means of transportation.
- Notification services of events: (1) in the field of network monitoring, physical and logical safety and security, (2) announcement of birthdays, (3) advertisements, (4) email which informs one of the presence of an email, (5) voice / fax which indicates the presence of a fax or voice message. (6) …
- The organization of television quiz by broadcasters,
- Communications at lower cost.
- …

This list is inexhaustive. As proof; authors of (SMS Tutorial, 2007) mentioned that SMS can be used to monitor stock market alert application, "a program is constantly monitoring and analyzing the stock market. If a certain condition is satisfied, the program will send a text message to the user's mobile phone to notify him/her of the situation". They also present SMS as a tool of remote system monitoring: "a program (sometimes with the help of a group of sensors) is constantly monitoring the status of a remote system. If a certain condition is satisfied, the program will send a text message to the system administrator to notify him/her of the situation. For example, a program may be written to "ping" a server regularly. If no response is received from the server, the program can send an SMS alert to the system administrator to notify him/her that the server may be hanged." Among the most important stakes of the future, the best success will be (NewNet SMserverTM, 1999) "to be able to use the handset as an extension of the computer" and it is what we try to prove with VeSMp protocol: to make of a GSM mobile terminal a true station for monitoring remote systems. William Enck & al (Enck et al., 2005) shows that it is possible to put a city of the size of Washington D.C. out of terrorist attacks using a simple SMS.

2.2 Process Monitoring

Process monitoring covers the set of functions which are necessary for the follow-up and maintenance of systems processes. It is necessary for a System or Network Administrator to initialize new services, to supervise the state of the global system of a company server or a given machine on a corporate network. It is also necessary to follow in a reasonable way the evolution of the performances and put an end to abnormal situations. One distinguishes the services of configurations, of test and diagnosis (faults management, maintenance, measurements of performances, etc.)

The Administrator needs tools to act and follow the activity of his system and to guarantee its availability at any time and place. Among these tools, we will distinguish the native tools from integrated solutions. Native tools are those furnished by the editors of the operating systems like telnet (Girondo Stéphane), ssh (De Wulf, 2001). The integrated solutions tools are those provided by proprietary editors or vendors such as CiscoWorks Solutions of Cisco Inc. (Cisco Works, 2006), OpenView of HP (Open View, 2006) and Soltice of Sun (Solstice Sun, 2006). VeSMp is classified in this last category of tools of remote administration. It allows the remote operation of the system in order to carry out technical inventories of the services/processes, their settings, their activation/deactivation; stop/restart from a telephone handset no matter its geographical location thanks to the roaming service of GSM operators.

3 THE VERY SHORT MESSAGE PROTOCOL (VeSMp)

A protocol of communication defines a number of formalisms that two or more remote entities must use to communicate together and cooperate to carry out a task or to exchange information each other. In the field of system and network administration for example, it makes it possible to develop software tools for system and network management in an efficient, coherent and standardized way. These tools allow the piloting of remote systems resources, real time monitoring and assistance with the diagnosis of breakdowns of systems. VeSMp forms part of the family of protocols making it possible to carry out actions in real time on the system to know its operating conditions (monitoring and diagnosis of incidents, measurement of real load, maintenance, control, information systems, etc) and react to them (activation/deactivation, stop/restart of the services/processes) (Postel and Reynolds, 1983). It can also allow deferred actions and estimate impacts on the system at a programmed moment.

3.1 Formal Description and Synopsis of VeSMp: Format of Use

VeSMp is a simple protocol based on SMS. It is a protocol of communication which we developed to give direction to messages that an application can interpret. In fact, the majority of actual system and network administration solutions as those mentioned above use TCP/IP protocol to perform the remote access to the corporate LAN before impact on system or network settings. The VeSMp protocol is based on GSM protocol and allows transforming an SMS to a valid system command. Its goal is to say much with least possible characters. VeSMp actually realizes five specific or proprietary commands: (1) `cmd` (for a system command), (2) `rtn` (for return) (3) `lgn` (for login), (4) `pwd` (for password) and (5) `lgt` (for Logout). Its synopsis or its format of operation is as follow:

```
##cmd CommandName [arguments]
[MachineName] [rtn]
```

We describe hereafter the syntax of the synopsis of a VeSMp message.

1. A VeSMp message is an SMS which starts with `##`.
2. A VeSMp instruction is all complete command that can be executed on an Operating System (OS) command line interface or shell. It starts with a succession of three letters (for example `cmd`) followed by the standard or real system name of the command provided by the OS accompanied with arguments: `cmd CommandName [arguments]`. An instruction describes the action to be executed. It is ended by the character `#`.
3. Instructions are separated from each other by the character `#`.
4. `CommandName` specifies the real or standard name of the command to be executed on the Shell provided by the OS of the machine `[MachineName]`.
5. `[Arguments]` represents the list of acceptable arguments by the command. If the command comprises arguments, they are inserted following the command separated from each other by the space character.
6. `[MachineName]` allows specification according to the naming conventions of the Network Administrator, the name of the machine of the network on which the command must be executed. It can be either an IP (Internet Protocol) address, or a DNS (Domain Name Service) name, or a reference symbol.
7. The command `rtn` specified at the end of the string allows a VeSMp-based application to send back to the user the result of the execution of the command.
8. The user has the possibility of pre-defining his instructions thanks to shortcuts or alias and thus of reducing the number of characters of the VeSMp message. We have baptized this extensible shortcut VeSM (for Very Short Message). It is thanks to this original mechanism that we can address a command that can exceed the maximum length of 160 characters of a conventional SMS.

We will hereafter illustrate the use of VeSMp protocol from an application by some examples.

Let us consider the following example:

```
##cmd dsk#rtn#cmd /sbin/service
mysqld restart#.
```

At the reception of this VeSM, the application will know that it is a VeSMp request. ***dsk*** (for disk; Linux command) will return (by a SMS) the partition statistics of the remote system, and ***cmd*** will execute the command which restarts (***restart***) the mysql server (***mysqld***) on a Linux machine. This command is in the system folder ***/sbin/service***. We propose here other examples to show the possibilities of VeSMp.

- `##cmd /sbin/service mysqld start#cmd /sbin/service httpd stop#`: this VeSM makes it possible to execute two commands on a Linux server: on a Fedora Core server, the first (`/sbin/service mysqld start`) starts the MySQL server and the second (`/sbin/service httpd stop`) stops the Apache server.
- `##cmd notepad.exe#`: this VeSM launches the **notepad.exe** program on all the Windows machines of the local area network (LAN).
- `##cmd gedit#`: this launches the text editor **gedit** on all the linux machines of the LAN.
- `##cmd firefox http://www.google.com#`: this VeSM uses firefox on any concerned machine to launch the google's web site; **firefox** is the command and **http://www.google.com** is the argument used by firefox.
- `##cmd du –sh /home#cmd df –h#rtn#`: here we see the possibilities of returning the result. The first command gives the statistics of use of the folder **/home**. The second posts the statistics of all the partitions on the linux server. But only the statistics of the partitions will be returned to the user by SMS because it alone is followed by an instruction ***rtn***.
- `##aaa#`***:*** this example of VeSM represents a contracted form or alias of the command to be sent. The subjacent command can exceed the conventional number (160) of characters of an SMS. The latter will be interpreted by a parser on the VeSMp server.

These examples illustrate some inexhaustive potentials of our VeSMp protocol. We describe in the following part the conceptual and management model of it.

3.2 Conceptual Model and Technical Architecture of VeSMp Protocol

Our model is based on the client/server model and the models of network management described in (Pugolles pp 829-876, 2002). VeSMp management

includes the system management which defines the exchanges of the whole information of management concerning the processes related to the resources used in the network. This information of management is stored in a database of information of administration called VeSMp Management Information Base (VeSMpMIB). This database consists of two essential tables. The purpose of this database is to store: (1) the VeSMp commands and (2) the information of management of the system or the network to be supervised.

A System administrator starting from a management entity (ME) sends a VeSMp message which will be forwarded by GSM radio channel to the SMSC. GSM radio channel ensures the service of remote operation (RO). The latter gives the VeSM to the Server or Manager of the management entity (VeSMpME) on the corporate network. The Administrator's terminal is the VeSMp client (VeSMpCl). It is also a management entity. More generally, VeSMpCl is all equipment used to send a VeSM and to receive an SMS. It can be all GSM terminals like a mobile handset or a computer connected to Internet or not on which an SMS-based application functions. The server management entity is a module installed on a machine of the network. The VeSMpMIB can or cannot be installed or configured on this machine. The SMSC communicates with the VeSMp server either by bluetooth, or by infra-red, or by data-cable or Null modem cable connected to a COM port, or by other compatible means. At the reception of the VeSM, the VeSMp server interprets it based on the information contained in the VeSMpMIB. If it is a valid command (see synopsis into 3.1), then an application entity (AE) takes on its execution. This execution will imply the calling of TCP/IP or OSI functions of management. If not, the client receives an SMS notification on behalf of the Manager of the application entity (AE). An AE must be configured and installed on each station of the network. The technical architecture of the conceptual and management model of VeSMp is illustrated in figure 1 below. It materializes the deployment of entities involve in the VeSMp protocol. Each entity of the network can have its VeSMpMIB. We can also configure one centralized VeSMpMIB for the whole of the entities.

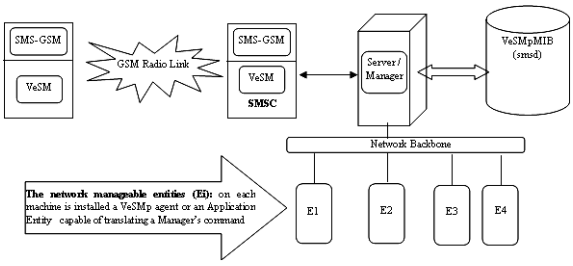

Figure 1: Technical architecture of the conceptual and management model of the VeSMp protocol.

3.3 The Algorithm of Management of VeSMp Protocol

The principle of management of VeSMp is simple. A Management Entity of VeSMp called VeSMpME is any device able to send and receive SMS. It can be a GSM radio terminal, an application installed on a computer or any compatible equipment for GSM able to carry out such a task. Communication takes place in the VeSMpME direction (located at the site of the remote client or mobile) towards the VeSMpMgr (VeSMp Manager) server connected to the SMSC. VeSMpMgr recovers VeSMp Protocol Data Unit (VeSMpPDU) which is a conventional SMS in a rough state. It takes it up to the level of VeSMp daemon (VeSMpd) which treats it and extracts VeSM. An applicative entity called VeSMp Application Entity (VeSMpAE) analyzes the VeSM and extracts the command and its arguments from them. The result is then given to a VeSMp agent (VeSMpAg) which makes the match with information of management in VeSMpMIB. The command is then given according to the context of local network management to the stack of TCP/IP (SNMP) or OSI protocol (CMIP). The same VeSMpAg recovers the result of the command, journalizes it in VeSMpMIB and gives a copy to the VeSMpMgr.

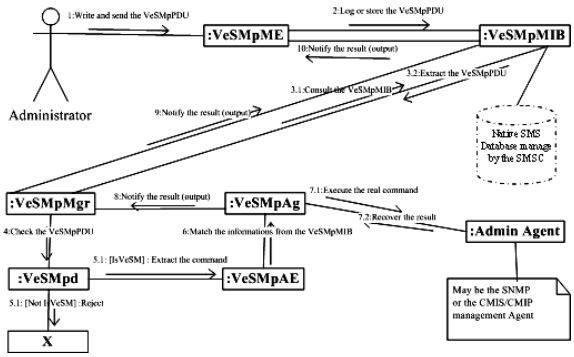

Figure 2: Diagram of interaction of the management of the VeSMp protocol.

The latter communicates with the SMSC which then notifies VeSMpME of the result (success or failure) of its request. The UML diagram of interaction shows by the figure 2 hereafter illustrates the collaboration between entities involve in the execution of the algorithm.

The figure 3 below materializes the architecture of deployment of VeSMp protocol.

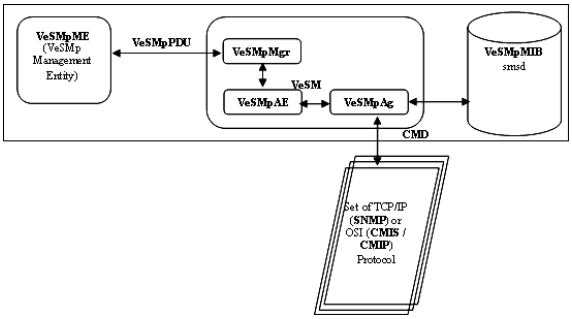

Figure 3: Architecture of deployment VeSMp of protocol.

VeSMp is an appraisable regular expression valuable by a context-free grammar (Pugolles pp 981-995, 2002). With this expression, we associate semantic actions to bring out a parser of SMS which, as output, produces an executable instruction on the command line system. We can by this confirm that a VeSM is a SMS of command. This means an SMS which originate real actions at the system level.

3.4 The VeSMp Protocol's Security Model

The VeSMp's security model associates three parameters which are: telephone number, login and password. It realizes three other supplementary commands: LGN (login), PWD (password) and LGT (Logout). These commands allow respectively to instruct the VeSMp manager to evaluate the user account composes by the login and the password. This is illustrated by the instruction:

```
##lgn AccountLogin#pwd AccountPwd#.
```

LGT allows ending an opened session by the instruction: `##lgt#.`

The first VeSM is used for authentication purpose. We call it the authentication VeSM. It permits to open a session. The session has a duration. This duration corresponds to the waiting delay of a VeSM by the VeSMp manager. If during this period of time no VeSM is detected, the VeSMp manager ends an opened session. If not, it reinitializes the session's counter. At the reception of the authentication VeSM, a VeSMpAE checks that the phone number is authorized if not it rejects the request. Then it checks if the account (login and password) extract from VeSM is an account of the domain: this is the identification and authentication process of the user in the directory. At any time, the Administrator can explicitly ends a session thanks to the command LGT.

The contracted form of VeSM messages is equally a level of security. This mode of codification of VeSMp instructions allows hiding the correct or real syntax and name of system commands of process remotely invoked.

4 DISCUSSIONS: INTEGRATION OF VESMP WITH STANDARDS SNMP AND CMIP

VeSMp is a system protocol for remote administration designed to be used in a company to improve the procedure of system administration and thus to increase the productivity of the company while making available the systems resources, no matter the geographical location of the Administrator. In this part, we show how this protocol is integrated into the international standard of system and network management like CMIP of OSI and SNMP of TCP/IP.

System monitoring is in the key idea of the VeSMp model. Its operation requires the presence of TCP/IP and/or OSI protocol. The exchanges are done between layers 7 (Application) of OSI model and 4 (SM-AL Short Message Application Layer) of SMS model (Pons, 2001). The data of system monitoring are brought up at the level of layer 7 - application of OSI model by the intermediary of an application entity. It is at this level that are elaborated, treated and taken the decisions of management. As we mentioned earlier, system monitoring is done by the logical entity VeSMpAE which in OSI model corresponds to a System Management Application Entity (SMAE) that generally must carry out these services. All the information of management are memorized in our management database VeSMpMIB. This corresponds to the Management Information Base (MIB) of models CMIP of OSI or SNMP of TCP/IP. The parser aims to translate VeSM into a system command. The execution of this command now will call upon the mechanisms of CMIP or SNMP management, all depending on the underlying protocol of management concerned. It also plays the

part of the supervising authorities of association ensured by the Association Control Service Element (ACSE) of the OSI model. This comparison is recapitulated in table 1.

Table 1: Illustration of the integration of VeSMp protocol into standard CMIP of OSI and SNMP of TCP/IP.

VeSMp	CMIP	SNMP
GSM protocols	ROSE	
our synopsis	SMASE	
Parser	ACSE	
VeSMpMIB	MIB	MIB
VeSMpAg		SNMP Agent
VeSMpMgr		SNMP Manager
VeSMpAE	SMAE	
VeSMpME		
VeSMpCl		
VeSMpAEl		

Notes about table 1: ROSE stands for Remote Operation Service. For VeSMp, ROSE is based on GSM protocols for SMS management. Our synopsis defines the syntax and the semantic of the information of management transferred by a SMS (SMASE). The parser plays the role of services of association (ACSE). The concepts VeSMpME, VeSMpCl and VeSMpAEl have no immediate correspondence. For more details about abbreviations, please see appendix.

After having described the VeSMp protocol, we present its model of management and its architecture. We also showed how it is integrated into the standard models of management like SNMP and CMIP protocol. By referring to the summary of the table 1 above, we can invariably use the same terms to refer to similar concepts, whether it is VeSMp, SNMP or CMIP.

5 CONCLUSION AND PERSPECTIVES

We are interested in the construction of effective solutions based on lower cost technologies: SMS. These are used in companies for tasks of notification or information in various fields (Wikipedia, 2006), (SMS Tutorial, 2007). We have proposed the VeSMp protocol, an original alternative of exploitation of the SMS service for monitoring systems processes and remote administration. It is a SMS-based protocol of communication. It allows the system administrator from the notification of an event or incidental system, to intervene on its system in the second which follows, no matter the geographical location. In this way he permanently remains in contact with the system or the corporate network. VeSMp makes it possible to render services to systems and corporate networks available at any time and place. The VeSMp protocol therefore makes it possible for companies to draw from the real advantages while making it possible for the administrators to remain virtually present in their companies thanks to their GSM terminal. VeSMp is a simple protocol of communication like telnet (Postel and Reynolds, 1983).

In its current version, VeSMp uses the association of three parameters: telephone number, login and password for securing messages. This association allows the authentication of the telephone number that emits the VeSM request, the authentication and the identification of the administrator to the system. It actually realizes five commands in addition to the possibility to invoke real system commands to perform administration tasks: (1) `cmd` (command), (2) `rtn` (return), (3) `lgn` (login), (4) `pwd` (password) and (5) `lgt` (Logout). We are studying a strategy that permits to guarantee the confidentiality and the integrity of VeSM. This will consist of giving answer to the question: how to integrate the cryptography into a VeSMp message.

We know that network management actions need to be undertaken in near-real time scales. At this level, a certain number of questions remain currently hanging: what happens if VeSMp does not succeed? How to insure the reliability of the protocol? What happens if the SMS service is slow in delivering the messages? The SMS message can be delay by the congestion or even by the fact that the recipient is temporally out of range from the base station. This returns within the framework of the quality of service (QoS) considerations within our protocol: treatment of the errors, management and fault tolerance, guarantee of success of a command, interruption of a running command, incident management and denial of service (DOS). Due to the noticeable limitations that GSM puts on the amount of data that can be gotten as feedback, another improvement consists in giving to the command **rtn** the possibility of providing a more detailed feedback code: is the command successfully executed? Which machine returns the feedback message? The specifications of the ping command (Packet INternet Groper) which is a benchmark for the administration is certainly going to inspire us in this idea.

The extension of this paper will concern the implementation, experimentation, and comparison of the VeSMp against other available solutions such as

telnet or OpenView. We are developing a VeSMp-based network administration tool: **VeSMp Network Monitor** (**VeSMp NetMon**) intended for the network monitoring and administration of the "Ecole Nationale Supérieure Polytechnique". It must be a portable tool based on open solutions like Java to guarantee the independence of the platform. In the medium term, our research will improve the quality of service offered and in the long-term we hope to make of VeSMp a standard protocol of system and network remote administration.

ACKNOWLEDGEMENTS

Many people contributed to reviewing this paper. It was a wonderful experience to discuss particular ideas with them. We are grateful to Dr. Guillaume Koum Dissake and Pr. Jean-Claude Derniame who reviewed the entire paper. Special gratitude goes to all members of LABORIMA and to our students Fritz Ekwogue, Yacoubou Mohamadou and Maïramou for experimenting with the VeSMp protocol.

REFERENCES

William Enck & al, May 2005. *Exploiting Open Functionality in SMS-Capable Cellular Networks*.

Finn Trosby, 2004. *SMS, the strange duckling of GSM*, Telektronikk

NewNet SMserverTM, 1999. *Wireless Short Message Service Tutorial, ADC Telecommunications.*

http://en.wikipedia.org, (14/08/2006). *Short Message Service*, http://en.wikipedia.org/wiki/Short_message_service.

Jérôme Pons, 2001. *Implémentation des services à valeur ajoutée dans un réseau mobile*, ENST, Rapport de stage.

Voutay - Dulong De Rosnay, 2000. *Le réseau Cellulaire GSM*, http://membres.lycos.fr/voutay/gsm/, (14/08/2006)

Roamware Intros Voice SMS, April 24, 2006, *http://www.lightreading.com/document.asp?doc_id=93061* (29/08/2006)

Guy Pugolles, 2002, *Les réseaux (Annexe B, La spécification de protocole, pp 981-995),* Eyrolles. 3iéme édition.

C. Demoulin, M. Van Droogenbroeck, 2004. *Principe de base du fonctionnement du réseau GSM*, Institut Montefiore Belgique, http://www.ulg.ac.be/telecom.

S. D. Noubissie Ngadeu, juin 2003. *Impact des services à valeur ajoutée dans les réseaux mobiles*, ENSPT Yaoundé Cameroun, Mémoire de fin d'étude.

http://www.gammu.org, 02/10/2006. *http://www.gammu.org/wiki/index.php?title=Gammu:Main_Page*.

J. Postel, J. Reynolds, May 1983. *Telnet protocol specification, Network Working Group RFC 854.*

Girondo Stéphane, *Architecture réseau GSM, GPRS et UMTS,* Mémoire pour mastère, www.girondo.com.

Martin De Wulf, juin 2001. *Un logiciel d'illustration des protocoles GSM et GPRS sur la voie radio*, Facultés Universitaires Notre-Dame de la Paix (Institut Informatique), Mémoire pour une maîtrise en informatique.

Guy Pugolles, 2002, *Les réseaux (Chapitre 31, La gestion de Réseaux,pp 829-876),* Eyrolles. 3iéme édition.

Cisco Works (Cisco Inc.), Oct 2006. *www.cisco.com/en/US/products/sw/cscowork/ps2425/*

Open View (Hewlett-Packard), Oct 2006. *http://h20229.www2.hp.com/.*

Solstice (Sun), Oct 2006. *http://www.sun.com/solstice/index.html.*

Short Message Service / SMS Tutorial, May *2007. http://www.developershome.com/sms/.*

APPENDIX

- VeSMp: Very Short Message Protocol.
- VeSMpMIB: VeSMp Management Information Base.
- VeSMpAg: VeSMp Agent.
- VeSMpMgr: VeSMp Manager.
- VeSMpAE: VeSMp Application Entity.
- VeSMpME: VeSMp Management Entity.
- VeSMpCl: VeSMp Client.
- VeSMpAEl: VeSMp Application Element.
- ROSE: Remote Operation Service Element.
- SMASE: Simple Management Service Element.
- MIB: Management Information Base.
- SMAE: System Management Application Entity.
- ACSE: Association Control Service Element.
- CMIS/CMIP: Common Management Information Service/Protocol.
- SNMP: Simple Network Management Protocol.