Controller for Mobile Control and Monitoring via Short Message Services

Rosen S. Ivanov[1]

Abstract – **The aim of proposed controller is to enable mobile access to small office and home office (SOHO) appliances via WAP and SMS commands. The appliances and sensors can be connected to RS 485 network or to local I/O ports. The software is written in C++ and allows sending and receiving of sort messages through mobile operator SMS Center (SMSC) or SMS to E-mail or E-mail to SMS gateways.**

Keywords – **Mobile Control, Mobile Monitoring, SMS commands.**

I. INTRODUCTION

Wireless Internet access is expected to be the next big market in telecommunication world. Mobile Internet combines two of the fastest growing industries: wireless communications and Internet. Mobile data transfer requires development of a lot standards, protocols and mobile network hardware/software. The big investments in this process leads to enlargement of price of mobile Internet services. The clients expected fast data transfer for attractive prices, but this is impossible at this moment. Wireless Application Protocol (WAP) was developed for turn a mass-market mobile phones into a network-based smartphone. Because of low data transfer rates and relatively big account prices WAP has many servers but still little clients. To increase data transfer rate WAP over General Packet Radio Service (GPRS) can be used if your mobile operator support this service. While we waiting for GPRS and Universal Mobile Telecommunication System (UMTS), a familiar wireless data transfer technology like Short Messaging Service (SMS) can be used in many applications. SMS is a globally accepted wireless service that enables the transmission of alphanumeric or binary messages between mobile subscribers via SMSC. It is low cost and easy to use solution for wireless connectivity.

II. HARDWARE DESIGN

The proposed controller (RS-MC 02) is stripped version of RS-MC 01 described in [1]. The latter allows mobile access to networked (RS 485 and Bluetooth™ interfaces) appliances and sensors from GSM with WAP. RS-MC 02 support only RS 485 interface, but can control and monitor appliances, sensors and SOHO devices via WAP as well via SMS commands.

[1] Rosen S. Ivanov is with the Department Computer Systems and Technologies, Technical University of Gabrovo, 4 H. Dimitar, 5300 Gabrovo, Bulgaria, E-mail: rosen@tugab.bg.

This work was supported in part by the Bulgarian's Ministry of Education and Science.

The design of proposed controller is based on Beck's System on Chip SC12 [2]. The SC12 is complete embedded PC with 80186 controller, DRAM, Flash Disk, IDE interface, Serial Interfaces, Ethernet controller, full TCP/IP stack with API for UDP and TCP sockets, many servers (HTTP, FTP, Telnet, PPP, UDP Config) and clients (PPP, DHCP). Real Time Operation System (RTOS) challenges maximum delivery from 16-bit CPU@20MHz in order to achieve high performance for TCP/IP communications and task switching. This architecture enables the reduction of size, power consumption, cost of controller and number of additional components as shown in Fig. 1.

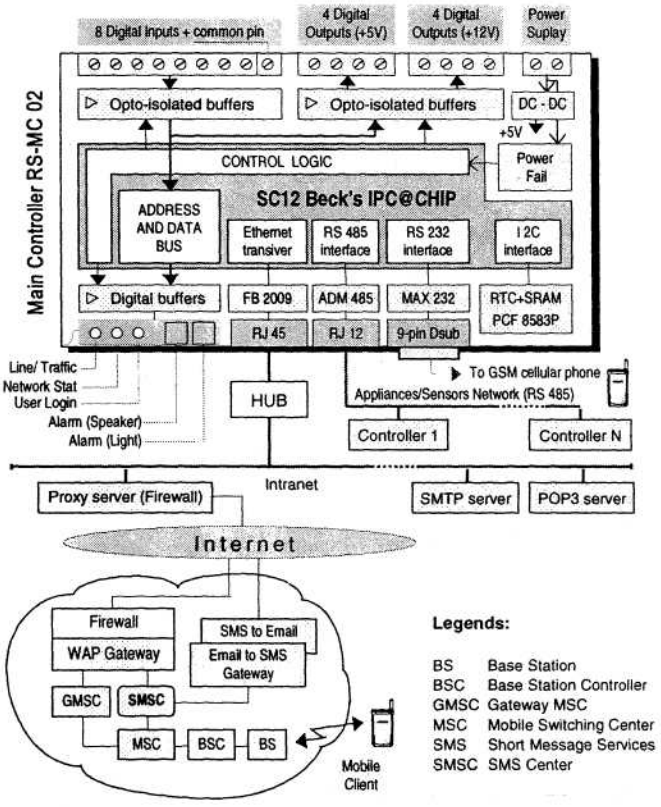

Fig. 1. Controller architecture and system configuration

III. SOFTWARE DESIGN

The software is build as a set of separate processes and tasks called managers. The objects of RTOS like semaphores, events and messages are used to guarantee synchronization between tasks and access to critical resources. An overview of the controller's software is shown in Fig. 2.

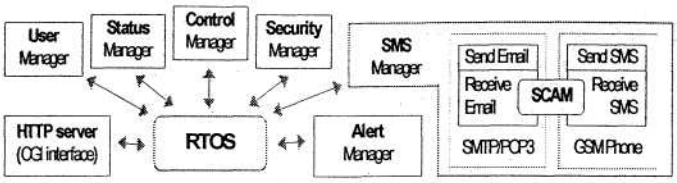

Fig.2. The basic structure of RS-MC 02 software

In order to enable control and monitoring via SMS commands the SMS manager is used. It allows SMS sending and receiving in two ways:

First, GSM phone connected to controller via V24 interface is used. In this case a set of AT commands [3] are used to send/receive short messages. SMS manager supports two ways of flow control: hardware (CTS/RTS) and software (XON/XOFF).

Second, capabilities of E-mail to SMS gateway, SMS to E-mail gateway and SMTP/POP3 servers are used. In this case if mobile user wants to send SMS command he must send SMS to SMS to E-mail gateway that converts SMS to E-mail and resends the message to Email address (first line of message). The SMS manager checks user PO Box periodically (5-10 sec) and if new message has been received starts SMS Command Analysis Module (SCAM). If the controller must sends SMS to mobile user (alert, report or reply message) it sends Email via SMTP server to E-mail to SMS gateway that resend information to GSM number included in E-mail address. When public gateways are used to send/receive messages any third party could monitor the message contents. The messages sent through SMSC are more secure.

A. Send SMS via GSM phone

First, select Protocol Description Unit (PDU) mode: AT+CMGF=0.

Second, use AT+CMGS command to send message: AT+CMGS=<lenght><CR><PDUdata><Ctrl+Z>, where length is number of octets in the data block.

For example, if we want to send SMS command "<rs> tvset on\r\n" the corresponding AT command is:

AT+CMGS = 28 13

00 11 00 0C 91 53 89 27 58 44 F5 ...

default SMSC phone number
SMS-SUBMIT
message ref.
GSM number: +35987285445
International number
len of phone number

00 00 A7 0F 3C F9 DC 07 A2 DB E7 65 3A E8 ED 6E 28 00 26

message: <rs> tvset on cr lf
message lenght in septets
validity period, 24h
select default coding scheme
protocol identifier
Ctrl+Z
end of data

B. Receive SMS via GSM phone

First, use command AT+CMGL=0 to get received unread (new) messages. If new message has been received GSM modem returns an answer in following format: +CMGL=<index>,<stat>,[<alpha>],<length><CR><LF> <PDUdata>, where:

- index is position of message in read/delete memory;
- stat is status of message after command (received read);
- alpha should be an empty string, but not omitted;
- length is length of data block in octets.

The following information is received when user sent the message containing command "<rs> tvset on":

+CMGL=1,1, ,40

07 91 53 89 08 00 03 F1 04 0C xx xx xx xx xx xx

len of SMSC info in octets
international #
GSM number: +35988000301
SMS-DELIVER
len of pnone # sender GSM phone number

... 00 00 30 20 50 01 12 30 20 0F 3C F9 DC ... 6E 28 00

protocol ID
default coding scheme
time stamp: 5 february 2003 10:21:03 GTM+02
message: <rs> tvset on cr lf
message len in septets

Second, call the SCAM (SMS Command Analysis Module) to check message.

Finally, delete the message, AT+CMGD command is used.

C. Send SMS via E-mail to SMS Gateway

We use following algorithm to send SMS via public E-mail to SMS Gateway:

1. Make connection with SMTP server (port 25). If OK goto 2, else retCode=(-1) and go to 10.
2. If server returns OK (220) goto 3, else retCode=(-2) and go to 10.
3. Send "HELO" command. If OK (250) goto 4, else retCode = (-3) and go to 10.
4. Send "Mail To:" command. If OK (250) goto 5, else retCode =(-4) and go to 10.
5. Send "RCTP To:" command. If OK (250) goto 6, else retCode =(-5) and go to 10.
6. Send "DATA" command. If OK (354) goto 7, else retCode =(-6) and go to 10.
7. Send message headers and body finished with single "." line. If OK (250) goto 8, else retCode=(-7) and go to 10.
8. Send "QUIT" command to destroy connecttion.
9. retCode = 0.
10. Close socket and return (retCode).

D. Receive SMS via SMS to E-mail Gateway

We use following algorithm to receive SMS via public SMS to E-mail Gateway:

1. Make connection with POP3 server (port 110). If OK go to 2, else retCode =(-1) and go to 11.
2. If server returns OK go to 3, else retCode=(-2) and go to 11.
3. Send "user" command. If OK ("+OK") go to 4, else retCode=(-3) and go to 11.
4. Send "pass" command. If OK ("+OK") go to 5, else retCode=(-4) and go to 11.
5. Check for E-mail or spam bombing (more than 2 messages received for last 5-10 sec). If no spams detected go to 6, else delete all invalid messages.
6. Send "list 1" command. If OK ("+OK") go to 7, else retCode=(-5) and go to 11.
7. Send "retr 1" command. If OK ("+OK") go to 8, else retCode=(-7) and go to 11.
8. Send "dele 1" command. If OK ("+OK") go to 9, else retCode=(-8) and go to 11.
9. Send "QUIT" command to destroy connection.
10. retCode = 0.
11. Close socket and return (retCode).

E. SMS Command Analysis Module (SCAM)

The SCAM allows to check mail box periodically for new messages. The new message is downloaded automatically and if its format is valid SCAM executes all SMS commands in message body. SCAM support 3 levels of protection:

First, if size of each incoming message is out of pre-defined range message is automatically rejected and deleted.

Second, SCAM checks message headers to ensure that SMS arrives from a valid sender. If sender identification (senderID) is not valid SMS is deleted.

Finally, each message has an identification number (messageID) and each command line starts with pre-defined command prefix (commPrefix). If messageId or commPrefix is not valid SCAM delete the message. MessageID is generated dynamically (id hopping) and controller sends new messageID with each reply SMS. Command prefix can be changed by administrator via WAP or SMS command or automatically if Security Manager reboots a controller.

IV. SMS Commands Description

SMS commands can be separated in following groups:

A. Change state of appliances or Get status of appliances and sensors

All appliances and sensors are recognized only by name. For this purpose Control and Status Managers used information in file NAME2INT.DAT. This file gives relation between name of each appliance/sensor and its corresponding interface, for example:

```
tvset N2 ID1    // TV Set is connected to RS 485 Network,
                // Controller=2, applianceID=1;
heater O4       // Heater is connected to digital output 4;
frontdoor I2    // Sensor for Front door is connected to
                // digital input 2.
```

Format of this commands is:

commandPrefix	applianceName or sensorName	actionID	[value]

Examples:

<rs> tvset on 3
Switch TV Set on for 3 minutes

<rs> heater prof 1
Starts time profile number 1 for Heater

<rs> alarm ?
Get status of alarm (ON or OFF)

<rs> frontdoor ?
Get status of Front Door.

B. Config or Get status of Alert Manager

Alert Manager checks status of pre-defined events. They are:

APPTIMEOUT - appliance timeout is elapsed;
SENSORSTAT - sensor status is changed;
FTPSESSION - FTP transfer is detected;
USERLOGIN - user login is detected;
USERLOGOFF - user logoff is detected;
INTRUDER - intruder is detected.

Last event (INTRUDER) is activated when 3 successive unsuccessful attempt for login or SMS commands has been detected. In this case security module disables all logins and SMS commands for pre-defined time interval to prevent "denial of service" attacks.

If an event was occurred Alert Manager informs pre-defined users via SMS, E-mail or local alarm (speaker and/or light). The relation between names of events and action (SMS, E-mail, BOTH, NONE) is described in file CHIP.INI, section ALERTS. Possible formats of this commands are:

commandPrefix	EventName	applianceName or sensorName	actionID
commandPrefix	EventName	userId	actionID
commandPrefix	EventName	actionID	

Examples:

<rs> SENSORSTAT all sms
Send SMS if status of a sensor is changed

<rs> SENSORSTAT frontdoor email
Send E-mail if front door opening has been detected

<rs> USERLOGIN john both
Send SMS and E-mail if user john is logged

<rs> FTPSESSION none
No action if FTP transfer is detected

<rs> INTRUDER speaker
Switch ON local alarm (speaker).

The local alarm (LED) is activated and if the controller loose connection with Intranet.

C. System Commands

This group of commands can be send only by user with administrator rights. They enable control of servers and controller rebooting. Possible format of this commands are:

commandPrefix	userPassword	senverName	actionID	[parameter]

commandPrefix	userPassword	actionID

Examples:

<rs> password HTTP dis 5
Diasable HTTP server for 5 minutes

<rs> password FTP ena
Enable FTP server

<rs> password reboot
Reboot a controller

The controller informs pre-defined mobile users with SMS when:

- SMS command is received and executed (reply SMS);
- alert event is detected (alert SMS);
- Intranet problem is detected - someone of pre-defined hosts (proxy, gateway, SMTP/POP3 servers) is not responding. In this case controller sends alert SMS via GSM phone connected to RS 232 interface.

V. CONCLUSION

It is vital that a new control and monitoring systems should allow remote or/and mobile access to appliances. The main advantages of proposed controller are as follows:

1. Controller can be used to make an extended range mobile control and monitoring, operable from anywhere in the world. According to required security WAP control, SMS control or both can be used.

2. Enhanced security features:

- automatic rebooting after fatal error or unauthorized access;
- all SMS commands are protected by a unique command prefix and message identification;
- all SMS commands are bi-directional - controller informs mobile user after execution of each command (reply messages) and for a pre-defined alert events (alert messages);
- only valid commands are accepted by the SMS Manager;
- anti-spam capabilities.

3. Very good prize to number of features ratio in comparison with similar controllers [4-6].

REFERENCES

[1] Ivanov, R., "A Controller for mobile control and monitoring of networked household and office applications", *International Scientific Conference UniTech '02*, Gabrovo, pp.194-197, Nov. 2002.

[2] www.beck-ipc.com.

[3] ETSI 07.05, Short Message Service and Cell Broadcast Service.

[4] www.pkd.no/io2000.htm, io2000 system, PKD Telecom.

[5] www.dialtelecom.com, co.s.a.t. CONTROL System.

[6] www.dobelt.de, DxDATA GSM-Control System.