A Secure System for Data Collection in GSM Networks

Martin Koutny, Jiri Misurec and Petr Mlynek
Department of Telecommunications, Faculty of Electrical Engineering and Communication,
UT Brno, 602 00 Brno, Czech Republic

Summary
This article is focused on the design and realization of secure long-line data connection in GSM network. The developing module Motorola MPC860 was used in this solution. This module is based on the operating system Linux. This operating system became the basis for the script development in the realization of automated long-line measuring system in GSM networks. The GSM modem Siemens MC39i is implemented in this system with a view to communication with mobile operator. This system enables data transmission by the help of GPRS technology. The secure communication is implemented by VPN connection between particular communication endpoints and the server.

Key words:
GSM, GPRS, secure transfer, VPN

1. Introduction

Systems of mass data collection are currently used for monitoring, administering final elements and collecting measured values. The increasing size of public data networks makes companies use these data lines. Many new problems appear in this repeach, especially in the security of data transfer. Fixed and wireless networks, which work with TCP/IP protocols, are the most widespread systems for these networks. The GSM technology [1], with its data transfers, is one of them. Currently, abundantly used generation is of these networks 2.5 generation; with its data transfer GPRS. Just by using this technology, measuring devices acquire features that they each in fixed connection. These features can be:

- mobility – it is possible to displace the equipment according to currently priorities of measurement;
- availability – almost 100% coverage of mobile signal enables to measure the values at places where it has not been possible up to now;
- price – the wireless technology reduces costs connected with the realization of network's infrastructure at the place of measurement.

Although this generation is one of the oldest, it is still the most widespread. And therefore it is evident that early security mechanisms of these networks cannot compete with modern cryptography attacks. It is especially the A5 cipher, which is used for encryption of data transmission between a mobile data terminal and the nearest BTS station [2]. After detailed exploration of the whole GSM transmission system it can be stated that this place is not the only one where it is possible to monitor the given transmission. The interface between BTS station and BSC controlled unit is not secured which results from the GSM network principles. It is evident that the danger of monitoring comes not only from network users but also from the very provider of mobile network. It is possible to communicate with the measuring centre after the GSM and the GPRS centre are connected to the Internet. The situation is illustrated in Fig. 1.

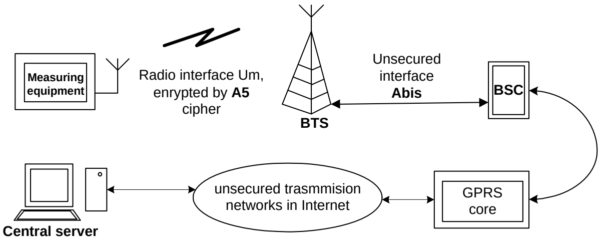

Measuring equipment
Radio interface Um, enrypted by A5 cipher
BTS
Unsecured interface Abis
BSC
Central server
unsecured trasmmision networks in Internet
GPRS core

Fig. 1: The security bandwidth scheme

2. Design of the system

Because the GSM structure is given it is important to seek security between terminated devices of the system. With regard to the GPRS technology which is a not commutated transfer working on similar principle as Ethernet, we can use the TCPIP model when seeking security. The application layer offers a range of new possible resolutions. One of them is to use one of the available tools for creating encrypted VPN connection and to apply it in the communication diagram. VPN connection accomplishes a safe and reliable communication between two or more points. The situation is shown in the Fig. 2.

- Measuring centre – the VPN server – the central point of the measuring network, where the VPN server and all the instruments needed for measurement from communication units are installed.
- Unsecured transmission network – this is a network needed for the connection of minimally two end points. If is made up of the Ethernet, Internet and GMS system of the mobile operator.

Manuscript received November 5, 2008
Manuscript revised November 20, 2008

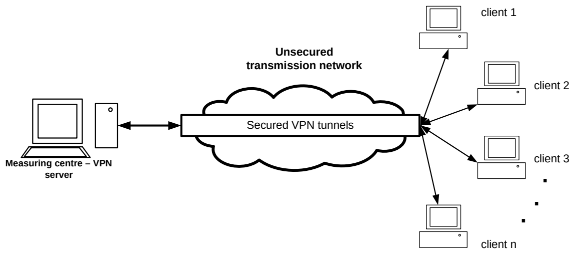


Fig. 2: System design for a secure data collection v GSM networks

- Clients – the communication units – they establish the VPN connection with the central server. Secure VPN tunnels are created in the network by establish these connections. The number of clients is given by the transmission band of central the server and subnet used.

3. HW realization

In order to realize the abovementioned suggestion, it was obvious that the hosting system should have a sufficient power basis for formation of tunnels, cryptographic operation and system administration. This is why the Motorola MPC860 [3] module is used. It is fully sufficient for implementing the Linux operation system. If is compiled and configured such that it allows an automated and secured measuring system. Two external memories are connected to the 32-bit microprocessor in this system. The first of them is a 4 MB FLASH memory, which is sufficient for the optimalization, design application and scripts. The second of them is a 4 MB DRAM memory, which is used as a cache memory for the operation system. The Ethernet interface and GSM interface are included in the unit for easier connection to the Internet. In our system the connection of a 100 Mbit the extension-line is used. The speed of extension-line is sufficient for contemporary standards and achievement of the system. Thanks to this features the module is used in range other realization [4][5].

The module of the Siemens MC39i modem [6] is connected by means of a serial line. The GSM or GPRS connection can be realized via the modem. The unit is connected to the Internet via GPRS; therefore it can establish a secure VPN connection with the measuring centre. Standard RS232 and RS485 are chosen as the communication interface for connecting of external measuring device. These communication ports are taken out to unit in a binate implementation. Therefore it is allowed to communicate with more than one device at a time. In this the way the resources are saved for the realization of other units.

4. SW realization

The Linux operation system is the basic link for the design and realization of new algorithms. Its functions and available program features provide a large area for development of necessary algorithms, which enable the realization of an automatic secure system. For the system to function it is necessary to configure and schedule correctly the instants when self tests will occur. These tests invoke in advance defined events in the case of problems. There are many events that can occur, e.g. the loss of GSM signal, the loss of VPN connection or bad initialization of SIM card, etc. In the Fig. 3 the basic block scheme of loading algorithm is indicated.

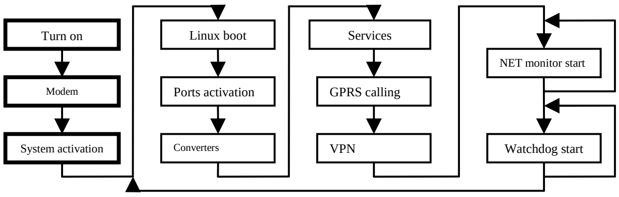
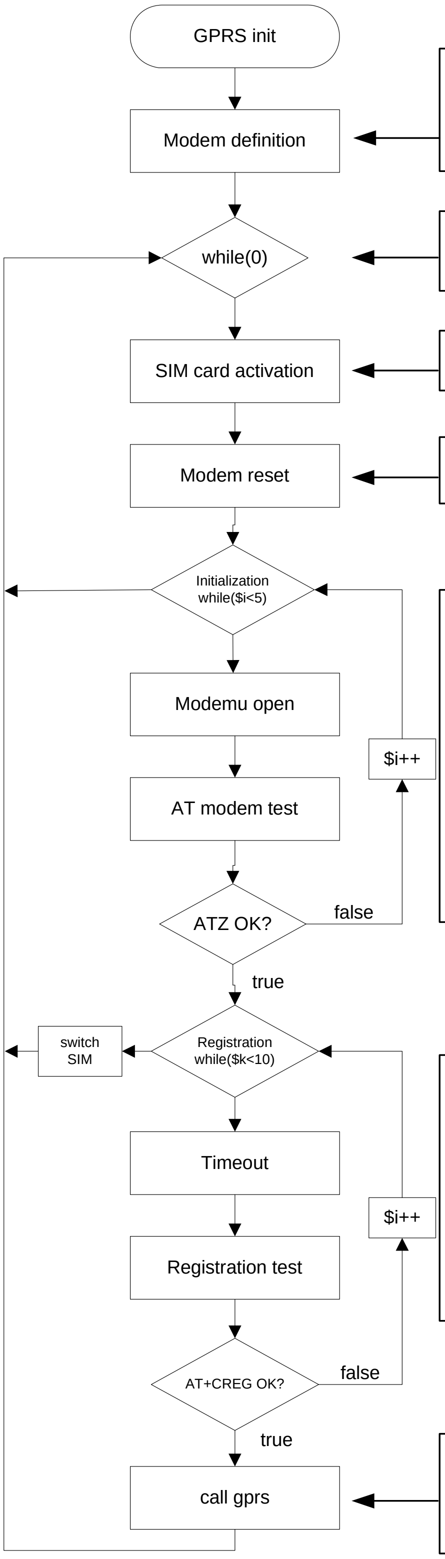


Fig. 3: The start system script

The MC39i modem is initialized after switching on the referential power supply and the booting of operating system takes place. The loading script is started as soon as the core is loaded. This script is turned on in the *respawn* mode. When the mode is closed, it ensures that it starts automatically again. The closing can be started manually through the instruction command kill or randomly by a mistake of the system. At the beginning of the script the available and used ports are activated. According to preconfigured setting the mutual transfer between them is activated. This setting of ports is can be programmed in configuration scripts through the remote administration via *ssh* or via the protected web interface. Afterwards the script is called, which tries to establish link GPRS connection (*GPRS_init*). When the link-up is successful, VPN connection (VPN init) is realized. The two scripts are also started in the *respawn* mode. The last called procedures are net monitor and watchdog. These procedures ensure automatic administration and restoration of connection, when the connection is broken.

4.1 GPRS init script

The connection GPRS is ensured by loading script GPRS init. This script takes care of the initiation, control and ending of GPRS connection. The flow-process diagram of the script is shown in Fig. 4.



At the beginning of the script, the modem interface is defined. In our example, it is a serial interface ttyS1, to which the variable MODEM_INTERFACE is assigned.MODEM_DEVICE

```
MODEM_DEVICE=/dev/ttyS1
```

The script then goes to an infinite loop, in which the necessary functions for GPRS control are included.

It is necessary to select the SIM card with which the connection is being realized

It is necessary to reset the modem with the SIM card. Thereby the card is initialized in the modem and the GPRS connection can follow.

Then the script goes to the next loop, in which it tries to activate the modem. The Linux command *stty* is used for this activation:

```
stty -F $MODEM_DEVICE
```

Afterwards the modem is tested for the basic AT command, which is called ATZ. In case of successful initialization the OK directive appears.

```
"ATZ" TIMEOUT 4 "OK".
```

If an expected answer does not followed in a defined time limit, the modem is reset and a new attempt is follows. In opposite case there is a new attempt to register the chosen SIM card in the network.

There are 10 attempts for this. In these attempts, the modem is asked about the registration validity by AT command AT+ CREG:

```
"AT+CREG?" TIMEOUT 4.
```

If the registration execution is not successful, system tries to test the modem registration again. After 10 unsuccessful attempts an alternative SIM card is assigned to the modem and the modem is rebooted. The whole procedure is repeated with the new SIM card.

If a successful connection is obtained, the system is connected to the internet network. This fact is verified by a *PING* order to the central server. Then, after obtaining a positive response, the system tries to establish to VPN connection.

Fig. 4: The design of GPRS init script

4.2. VPN init script

After connecting of the communication unit to the GPRS network, the establishment of VPN connection with a remote server is attempted. The OpenVPN program [7] is compiled in the unit for this purpose. In dependence on the server configuration the unit has to prove, that it is a valid participant in the communication. There are many methods how to prove the client's valid authentication. For our case the authentication of the unit is guaranteed by the client's valid certificate and by the knowledge of the common password. After a successful authentication and the establishment of cipher connection the process of connecting is finished and the system changes into the status of safe data sending and testing of connection.

4.3. Net monitor and watchodog

After establishing encrypted VPN connection, it is tested in the system. This is important for a flexible response to potential changes. For this testing, the script net monitor is realized; the script is demonstrated in Fig. 4.

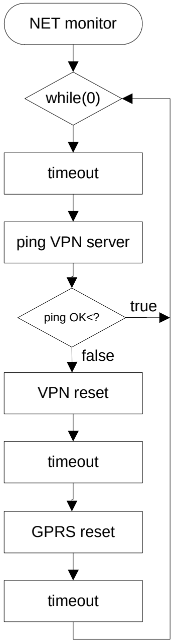


Fig. 5: The design scheme of script for connection test

The script includes the endless loop, which includes the instruction command ping. When the realization of the ping instruction command is successful, the cycle merges into the sleep status. After its ending the ping instruction command is called again. When the realization of the instruction command is not successful, the instruction command for closing the VPN connection and the GPRS connection is called:

- `killall openvpn`
- `killall pppd`

Because the script for GPRS initialization and establishing the VPN connection was at the beginning started with the marker respawn, the restoration of connection is automatically attempted. This guarantees that the system automatically tries to connect to the server also in the case that the signal is lost. The watchdog is started as an upgrade of net monitor. The watchdog stops the system or invokes the reboot process in the case of critical mistake. In this case, all the above mentioned process is repeated.

5. Testing of data throughput, connection stability and length of equipment response

Because the system is designed for online data transfer, it was subjected to short-time tests of the data throughput, connection stability and length of equipment response to variable lengths of packets included in the ping command. For testing the throughput this unit was connected to the measuring equipment. This equipment was a measuring instrument for measuring and long time recording of electric currents, voltages, effective and idle currents, and energies in the power networks. Thanks to the possibility of online measuring it can record and transfer the events (e.g. voltage drops, voltage boost etc.) in a determined time period. This period was defined as 4 s. This means that there was one measurement per 4 s. The results of these short-term measurements are in the table bellow.

Table 1: Test of data throughput and connection stability

Time [s]	4
Number of measurements	900
Successful measurements	892
Error rate	$9\cdot10^{-3}$
Transmitted data [kb]	2345
Received data [kb]	1752

This short-time test shows that the communication unit is able to respond flexibly the measuring centre commands. It was proved in the test that the system did not process circa 1% of data. This is perhaps caused instant of time (4 s) or the by mild decline of GSM signal.

6. Conclusion

In the paper the proposal of a unicast solution of the system of mass data acquisition for online measuring was described. The connection with the central point of network is established for every participant, which results from the character of the unicast communication. This connection was realized with the help of the GPRS technology. This technology is quite obsolete, its security mechanisms do not agree with the requirements for the given realization. For this reason, a security upgrade was realized at the application level of TCP/IP model. This upgrade is realized by the establishing an encrypted VPN connection with the help of the program OpenVPN, which was compiled in the system.

In the article, a possible method for realizing the solution was described. This solution is based on a relatively efficient system, which was made on the basis of the Motorola power PC microprocessor and the MC39i modem with two SIM cards. The Linux operating system was compiled in this system. Linux is configured such that it enables nothing a real-time automated safe data acquisition system. The functions and the available program facilities provide enough space for the research into and development of useful algorithms; thus it has the potential for further exploitation

The realization of designed algorithm was successful, so it was possible to test this realization in the real situation. The system is established specially for online measuring, so the system was exposed to a short-term exercise test. Table gives the results of measuring. It was proved in the test that the system did not process circa 1% of data. This is perhaps caused by the short time moment (4s) or a slight decline in GSM signal.

In conclusion, it is necessary to say, that in the case of using GPRS connection, the system is not suitable for complicated data transmission. It is caused by used technology used which in the present realisation reaches a maximum speed of only 84 kbps and relatively long response time.

Acknowledgments

The paper was written within the Czech Academy of Sciences project No. 1ET 110530523 and MPO FT-TA2/073.

References

[1] HEINE, Gunnar. GSM Networks : Protocols, Terminology and Implementation. 1999. pp. 416. ISBN 0-89006-471-7.

[2] J. Golic, Cryptanalysis of Alleged A5 Stream Cipher, proceedings of EUROCRYPT'97, LNCS 1233,pp.239{255, Springer-Verlag 1997.

[3] Freescale Semiconductor. MPC860 PowerQUICC™ Family : Hardware Specifications. 8th rev. edition. 2007. pp. 80.

[4] PRZYWARA, A., KUSCH, R., NAUNIN, D. Real-time operating systems on small embedded devices for industrial control and communication. In Industrial Electronics Society, 2003. IECON '03. 2003. pp. 2047-2053. ISBN 0-7803-7906-3.

[5] LI, Bo, ZHANG, Jian-wu, XU, Xiao-rong. Design of Data Acquisition System on Embedded Linux with Dual Port Asynchronous RAM. In Industrial Electronics and Applications. Singapure, 2006. pp. 1-4. ISBN 0-7803-9514-X.

[6] Siemens. Wireless Module MC39i : Standard GPRS connectivity without complexity. 2005. pp. 4.

[7] OpenVPN [online]. 2008 , 2008 [cit. 2008-06-06]. Available from <http://openvpn.net/>.

Martin Koutny received MSc at the Department of Telecommunications at the Faculty of Electrical Engineering and Computer Science at Brno University of Technology in 2007. He is engaged in research focused on mass data collection systems.

Jiri Misurec received MSc in 1985, Ph.D. in 1991 at the Faculty of Electrical Engineering and Computer Science at Brno University of Technology. In 2007, he received Assoc. Prof. degree at Brno University of Technology. His current research interest includes a data collection in PLC communication.

Petr Mlynek received MSc at the Department of Telecommunications at the Faculty of Electrical Engineering and Computer Science at Brno University of Technology in 2008. He is currently a PhD student at the Faculty of Electrical Engineering and Computer Science at Brno.