INNOVATIVE INFOTECHNOLOGIES
FOR SCIENCE, BUSINESS AND EDUCATION

SCADA SYSTEM IN GPRS NETWORKS: ENGINEERING AND REALIZATION

Aistė Andrijauskaitė [a] , Feliksas Kuliešius

Department of General Physics & Spectroscopy, Vilnius University,
Saulėtekio 9, korp. 3, LT10221 Vilnius, Lithuania

Received 4 July 2009, accepted 2 November 2009

Abstract. The article discusses SCADA systems in GPRS networks, their engineering concepts and realization possibilities. The first part of the article describes SCADA systems in general: the main elements and their functions are introduced. The second part discusses the advantages and disadvantages of various data transmission systems. GPRS networks are selected as the most appropriate medium to be used in SCADA systems. Consequently, GPRS networks and their relation with GSM networks are introduced as well. The last part discusses the minimum hardware and software requirements for realization of the most basic SCADA system.

Keywords: SCADA; Telemetry Systems; GPRS; GSM.
Short title: SCADA systems

Introduction

New technologies have become increasingly important in our lives and can be used in more and more different areas. One of the most important questions is how to observe remote events, which are located several hundreds or thousands meters away, and how to quickly and timely respond to system changes. For such data monitoring and collection SCADA systems were designed. These systems may be implemented in various fields – from industry to housing. The main purpose of such systems is to monitor, gather and analyze data. The system processes the received data all the time, as a result it could take on appropriate actions, for example, to send specific tasks to controllers or inform relevant people or instances about the situation when deviations are noticed.

Data transmission media in such systems may vary: wireless communications, cables or telephone lines. It is shown that the most appropriate medium to use for communication in SCADA systems is GPRS networks due to its reliability, ubiquitous character and pricing. Selecting this transmission medium, SCADA system becomes independent of distance, so remote devices can be monitored practically from any location. Consequently, GPRS service would be overviewed.

The aim of this article is to review the operation principles of SCADA systems – i.e. i) to discuss the way how data is transmitted in GPRS networks and ii) to review the main software and hardware technologies which are needed for realization of such telemetry systems.

1. SCADA Systems

Supervisory Control and Data Acquisition systems (SCADA) could be described as data management systems, which enable operators to monitor and control processes in remote areas.

Implementation of SCADA system saves time and money, because it is not necessary to go to remote sites for data collection or to check the functionality of the system. Real time data and system management, automatic report generation, system errors elimination and many other functions become possible. This is only a small part of all benefits that are provided with today's SCADA systems.

SCADA systems have become popular in about 1960, when the need for effective remote installation and control maintenance appeared. SCADA system is an electronic system which manages the input / output signals transmitted between the main station and remote devices. The master station would receive data through a telemetry network and then store it in the database

[a]Corresponding author, email: *aisteand@gmail.com*, phone: +370 671 47247

of mainframe computer [1].

Distributed control systems (DCS) were developed in 1970. It was used to control separate remote subsystems. When microcomputers were invented, it had become possible to distribute process control among remote sites. Further inventions enabled DCS systems to use *programmable logic controllers* (PLC), which may be programmed to control the remote sites.

Since the Internet takes the huge part in everyday lives and it could be used practically everywhere, SCADA systems also could use the certain ports to download information or control a process. Of course, security is an important factor that should be considered, so consequently all necessary security measures should be implemented in such systems.

Today's SCADA systems have many ways of realization. It can be used not only for process automatization in various industries, security systems of buildings, surveillance, but also for scientific purposes, i.e. for measurements, analysis and planning, also for weather forecasting, and for many other data acquisition/control systems.

2. Functional structure of SCADA systems

SCADA system performs four main functions: a) data collection; b) networked data communication; c) data presentation; d) control. These functions are performed by four SCADA system components.

1. *Sensors* (digital or analogue) and *controllers* that are directly associated with the managed system.
2. *Remote Telemetry Units* (RTUs). These are small computerized units, located in particular sites. The main function of these units is to gather data from sensors and send it to the main computer or, conversely, to send control commands from main station to controllers. Besides, RTU can perform routine local device manipulation.
3. *SCADA master units*. This is the main computer station consisting from few to several main computers that serve as the central processor of SCADA system. These units allow operators to monitor system events and manage control by analyzing received data. Sometimes these units are called *Human-Machine interface* (HMI) or *Human-Computer interface* (HCI).
4. *Data communication network* connects master SCADA units with Remote Telemetry units.

The simplest SCADA system can be imagined as a single circuit that notifies only about one event. For example, there is a machine which produces any kind of device. Every time when a device is finished it turns on the switch, which turns on the light indication in the control panel on the main computer station. This light indication informs a human operator that device has been completed.

Of course, a real SCADA system can perform much more actions and monitor much more remote sites in longer distances, but the main principle remains the same.

2.1. Data collection

A real SCADA system controls hundreds or thousands of sensors. Some of these sensors monitor the system behavior when some new objects appear (for instance, observes the water flow to the reservoir), the others - when objects are removed from the system (for example, measure the valve pressure, when water is released from reservoir).

Some of these sensors measure simple events that may be linked to the switch states on / off (so-called digital or discrete data). Other sensors are specialized to monitor more complex situations, where accurate measurements of gradually changed parameters need to be made (so-called analogue sensors). These types of sensors can analyze plenty of data variations, for example, voltage and current changes. Such sensors usually are designed to measure the temperature, flow, level of liquid in the reservoir or other alternating factors. The majority of these factors are defined with top and / or bottom levels.

Let's suppose the desirable room temperature is between 20 and 24 degrees of Celsius. If it becomes lower or higher, a threshold alarm is received, which informs about the unwelcomed temperature in the room. In more advanced systems analogue sensors have several types of threshold alarms.

2.2. Control

SCADA system is not limited only to collect and process data over the large distances, but also can control the remote devices. Suppose we have the control panel button. When the button is pressed, a signal is sent to remote devices to perform a particular action. In real systems this process frequently is automated and is performed at threshold levels. The main computer station monitors all devices (or particular factors) and when notices the deviation, immediately takes the particular action, for instance, sends appropriate commands to restore the previous normal state. In this way the system can operate without human interference, but also it is possible to adjust working processes manually.

In reality, SCADA system automatically controls various types of industrial processes. For instance, if the pressure is too high in the gas pipeline, system automatically opens the additional valve. Electricity generation can be adjusted to meet the appropriate energy requirements. SCADA system simultaneously can control a huge number of remote sites located in large distances.

2.3. Data presentation

Operators can observe data in the specific main computer station. Also it could be called *Human machine Interface* (HMI) or *Human Computer Interface* (HCI). The main functions of such computer station are as follows.

1. Constantly control all sensors / controllers and notify about alerts to human operator, i.e. when the control factor no longer satisfies the conditions or states which were set.
2. To present the whole view of all the system and responses to operator queries in detail.
3. To process the received data from sensors: maintain journal of reports and summarize history of events.

2.4. Data communication

SCADA data is encoded in concerted protocol format [2]. Older SCADA systems depended on closed proprietary protocols,

but today the trend is to open, standard protocols. Sensors and controllers are very simple electric devices that cannot generate or interpret communication protocol on their own [2]. For this reason *Remote Terminal Units* (RTUs) are used. RTUs encode sensor signals into protocol format and forward data to the main computer station. When RTUs receive control commands from the main station, they transmit appropriate manipulation signals to controllers.

There are many ways how data could be transfer in SCADA systems: Internet networks, leased and phone lines, wireless communication. Even when using the Internet, the last mile connection is needed. Usage of cables is not one of the best options, especially if large transfer distances are needed. In this situation additional optical cabling or repeaters should be located to strengthen the signals. Implementation of such network requires additional expenses and time. Wireless networks from this point of view are more simple and rational: the sites where cabling is problematic could be reached and this saves implementation expenses and time, which are great advantages of SCADA systems. Especially topical are structured wireless data networks, based on common place services, such as GSM, TETRA, APCO etc.

GPRS service is wireless data technology used all over the world. Besides, these networks are trusted and secure. One of the reasons why these networks have expanded is because of already existing GSM networks. GPRS networks are based on the architecture of GSM networks, so in order to create GPRS networks only few new improvements (installion of several new elements) in GSM networks need to be done by its operators. Consequently, there is no need for clean new network implementation, only already existing networks are used and improved.

Another advantage of GPRS is that the price of service depends not on the connection time, but only on quantity of data that was transferred due to connection. This is very convenient and practical – devices can be always on-line, what guarantee immediate reaction of system.

3. GPRS system

General packet radio service (GPRS) is a packet oriented mobile data service available to users of the 2G cellular communication systems GSM, as well as in the 3G systems. 2G cellular systems combined with GPRS are often described as 2.5G, that is, a technology between the second (2G) and third (3G) generations of mobile telephony. It provides moderate speed ($56 \div 171.2$ kbps [3], which is quite sufficient for usually small amount of data in SCADA systems) data transfer, by using unused time division multiple access (TDMA) channels in the GSM system. GPRS is a best-effort packet switched service originally standardized by European Telecommunications Standards Institute (ETSI), but now by the 3rd Generation Partnership Project (3GPP).

3.1. GSM networks

In 1982 the European Conference of Postal and Telecommunications Administrations (CEPT) rounded up a team of people and called it *Groupe Special Mobile* (GSM). The aim of this team was to create a new telecommunication standard in Europe.

13 European countries signed a memorandum of agreement in 1987 that the implementation of GSM networks would be completed until the year 1991. European Telecommunications Standards Institute (created in 1988) was responsible for creating the suitable technical requirements for European standards. In 1989 the sense of acronym GSM was changed. The meaning of GSM became *Global System of Mobile Communications* (GSM), because the concept needed a name which would be more in line with reality.

The first commercial GSM call was made in Finland on the 1st of June in 1991. The installation of the second stage of GSM networks continued till 1995. Main focus of this installation was a more effective and smooth transmission of voice data and services related with it. During the advanced second stage installation, the purpose and tasks had changed: the main focus was set on data transfer.

3.2. The mobile communications system

Mobile communications use radio lines and networks. The service sector in a mobile communication system is divided into many small zones, called cells. Each cell is connected with neighbor cell by cable and such network was called cellular network of communication [4]. Every cell has its own base station. The capacity of such system, i.e. the amount of users which could be served, may be expanded using multiple radio channels in different cells, where there is no interference. On the other hand, cellular systems require complex procedures for its own users' registration and call management realization, especially when users migrate from one cell to other.

Cell is the area covered by one base station antenna. The form of this area depends on what type and layout of antenna is used. By changing these features' triangle, rectangle and hexagon shape of a cell can be received. Hexagon shaped cell is the most optimal for communication. The main cell could be divided into N small sectors, with the size equal to 1/N of the main cell size. Such sectors are called microcells. This method is used in cities where density of subscribers is very high. If radius of cell is only tens of meters, then it is called the picocell. Size of cell can be easily reduced, if the base station antenna height is reduced.

3.3. Mobile communications organization

There are two different radio frequency channels for mobile communication organization used in Europe: $890 \div 915$ MHz – from mobile device to the base station and $935 \div 960$ MHz – from base station to devices. GSM additionally can use another – 1800 MHz frequency band. Cells of low frequency are larger, but have less frequency channels.

The main three possibilities of channel distribution could be formulated as follows: a) *Frequency Division Multiple Access* (FDMA); b) *Time Division Multiple Access* (TDMA); c) *Code Division Multiple Access* (CDMA).

The radio channel in FDMA occupies a relatively narrow bandwidth. Signals of different transmitters are sent in different frequency channels. Band filters are used to reduce the interactions of two adjacent channels. FDMA method is used in the first-generation analogue cellular communication systems.

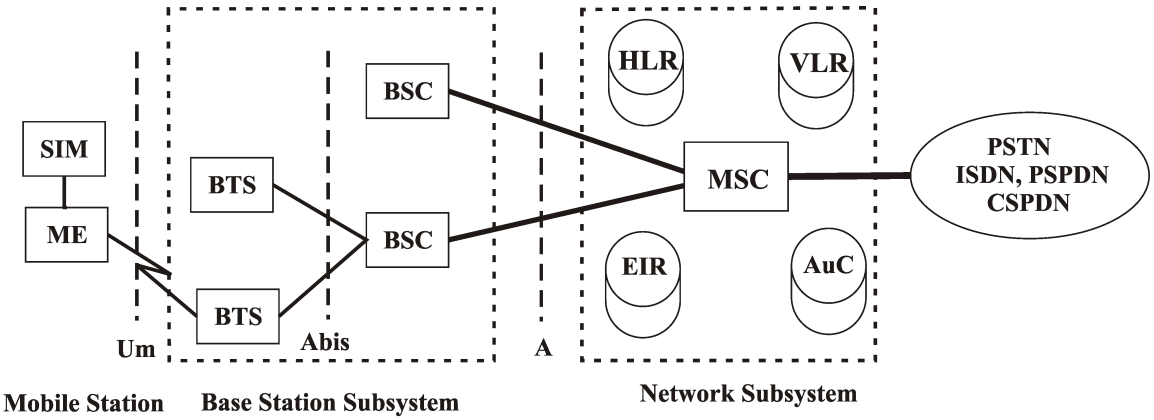

Fig. 1. GSM structure.
MS - Mobile station; SIM - Subscriber‘s ID module; ME - Mobile equipment; BS - Base station;
BTS - Base transceiver station; EIR - Equipment identity register; NS - Network subsystem; BSC - Base station controller;
AuC - Authorization centre; HLR - home location register; VLR - visitor location register; MSC - Mobile stationary centre.

TDMA system users can use the same frequency channel - however it could be occupied only during different time slots.

Since signals do not overlap in time, outgoing signals of a particular subscriber can be easily distinguished from other subscriber signals, by turning on receiver during the necessary time slot. The intervals of connection time could be shortened to boundaries which are allowed for the network synchronization. The systems which use TDMA usually have reserved intervals of $30 \div 50$ microseconds between adjacent channels. This means that all user terminals must be synchronized with their own base station at least with half accuracy of these reserved intervals. This task is completed when one of the communication channels translate the sample synchronization signal of the base station. TDMA is used in the second generation of digital mobile communication systems. It is also installed in GSM. Different frequency channels (carriers) are separated one from the other with 200 kHz band intervals. Each carrier may be transmitted in eight TDMA time slots. The length of each channel is 577 μs. GSM data block length consists of eight such time slots – 4,62 ms.

The third technology of channel distributions is CDMA. It appeared almost simultaneously with TDMA. In the beginning, it used more expensive equipment, as a result it took more time until it was started to use. In CDMA technology each signal is corresponding with different random binary sequence. This sequence modulates the carrier and extends its range. If the emitted radio signals of CDMA transmitter are observed from the outside, they will appear as a noise – over time, one or other component of spectrum is strengthened with no visible order. The transmitted information in this noise can only be acquired by someone who possesses a correlator in the receiver which is managed by exactly the same binary sequence as it was in transmitter. The communication system of so called *spread spectrum* protects from listening and inhibition much more than traditional narrow band radio communication systems [3].

3.4. GSM Network Structure

GSM network can be divided into three main parts (see Fig. 1).
1. *Mobile station* (MS) - phone or modem of network subscriber.
2. *Base transceiver station* (BTS) controls the radio communication with mobile station. BTS via *base station controller* (BSC) connects to *Mobile switching center* (MSC).
3. *Network subsystem*. The main part of this subsystem is MSC which performs the authentification process and call connection between fixed or mobile subscriber.

The mobile station and subsystem of the base station communicates over the U_m interface, also known as the *Air Interface* or *Radio Communication*. The MSC communicates with base station subsystem through A interface (see Fig. 1).

3.5. GPRS networks

GPRS networks are the improvement of GSM network infrastructure, which ensures the transfer of packet data. This means that GPRS has taken over the same cellular system networks, which allow voice calls. As a result a voice call service using GPRS is available anywhere. This service is also available abroad, since most operators have made contracts.

GPRS is defined as a packet data network, where the base station is used only when users send or receive data. The radio channel is not occupied or booked for any user for a particular time. Several users can use the same channel, i.e. the large number of users share the same bandwidth. The exact number of users depends on what application number and data quantity.

GPRS is based on IP protocol and allows users to access various services, for example to check e-mails, access internet or intranet, communication sites, chat, etc. Bandwidth of GPRS is between 9.05 kbitps to 171.2 kbitps [3].

GPRS connection could be described with motto: *Always on Always connected*. This means, that if you once connected to GPRS network, you can stay connected for the whole day or week or the rest of your life. The charge of GPRS service depends on what quantity of data subscriber has downloaded and uploaded, not on connection time like in GSM networks [5]. GPRS creates substantial benefits to service providers and consumers, because radio resources are more effectively used, i.e. the channel is occupied just for a while, only to transfer data packets. That is why the lower price of connection is charged.

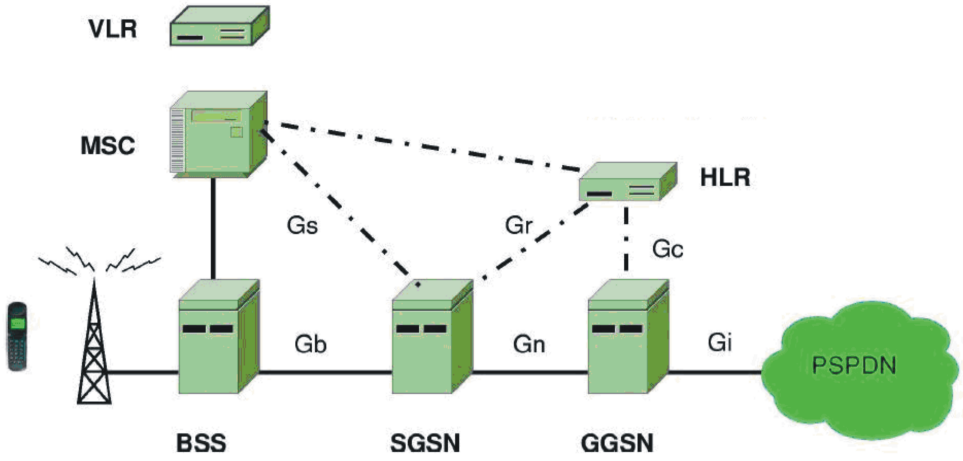

Fig. 2. Structure of GPRS networks.
BSS - basic station system; GGSN - Gateway GPRS Support Node; HLR - Home location register;
MSC - Mobile switchboard center; PSPDN - Public service packet data network;
SGSN - Serving GPRS Support Node; VLR - Visitor location register.

3.6. GPRS network structure

GPRS has been based on the GSM network standard by adding several new functional elements. In this way a system with defined functional capabilities and internal network operations has been created. The structure of GPRS network is shown in Fig. 2.

The following standardized network interfaces are also shown in the layout of GPRS network (Fig. 2).

1. **Gb** - sends user data and signaling messages to / from the SGSN.
2. **Gn** – GPRS network framework. IP LAN / WAN technologies are used for installation, providing a virtual connection between the SGSN and GGSN.
3. **Gi** – the boundary between GPRS and external networks. Each packet is routed by its unique access point name.
4. **Gr** – the interface between *Home Location Register* (HLR) and the SGSN. Allows connection to the subscribers' information.
5. **Gs** enables cooperation between GSM and GPRS networks.
6. **Gc** is the interface which enables GGSN to connect to the visitor location register.

Several new elements were installed in GPRS networks [6].

1. *Serving GPRS Support Node* (SGSN) is responsible for delivery of packet data to and from mobile stations, i.e. the best path selection and transmission (routing), mobile and logic connections management (connected / disconnected devices and location management), authentication functions. SGSN location register stores information of all registered GPRS users (for instance, in which cell the user is right now). This information is stored in visitor location register (VLR)) and users profile (for example, *International Mobile Subscriber Identity*, address (es) used in packet data networks).
2. *Gateway GPRS Support Node* (GGSN) works like an interface between the GPRS core network and external data networks. GGSN converts the received GPRS packets from SGSN to particular Packet data protocol (PDP), e.g. IP and sends it to the outside packet data network. If data comes from an external network then the address of the packet data protocol is converted to GSM recipient address. Redirected packets are sent to the SGSN. For that reason *Gateway GPRS Support Node* stores addresses and profiles of existing SGSN users in *Home Location Registers* (HLR). HLR is the information storage of all registered subscribers on that network. Each user must have at least one GPRS subscriber entry. GGSN is responsible for distribution of IP addresses and authentification, also. The unique access point name (APN) is assigned to each external network and is used when users want to connect to a particular network.
3. *Base Station Subsystem* (BSS) is adapted to recognize and send users' data to SGSN.
4. *Packet Control Unit* (PCU) is a part of the base station controller (BSC), which controls and manages distribution of GPRS radio recourses to mobile subscribers.

Other elements (not presented in Fig. 2) are as follows.

1. *Charging Gateway* (CG) registers any activity related with network, i.e. data transmission, loading conditions changes, quality of Service changes, the end of GPRS session (types of PDP packets). The main functions of CG are as follow: i) to collect records of GPRS data from network nodes; ii) storage of intermediate data records; iii) buffer and forward data records to the billing systems.
2. *Domain Name Service* (DNS) allows users to initiate connection to the appropriate network. It relates APN with IP addresses stored in GGSN.

3.7. Classes of Mobile stations

GPRS mobile station can operate in one of three classes.

1. *Class A. Mobile station* (MS) can use both GPRS and GSM services simultaneously. The consumer can make and / or receive calls using both services at the same time, for example,

consumer can receive a GSM voice call and GPRS data packets at the same time.
2. *Class B.* MS can use both GPRS and GSM services, but not simultaneously, i.e. if consumer accepts a GSM voice call at the same he cannot receive GPRS data packets.
3. *Class C.* MS could use only one service: GSM or GPRS, it cannot perform several operations at the same time. The choice of service is determined manually.

The MS of second GSM stage uses one uplink and downlink channel at a time. In GPRS service it is possible to have multiple time slots at a time, for instance, MS can operate in 2 time slots with two uplink and downlink channels. When MS uses multiple time slots it belongs to multitime slot class.

4. GPRS coding schemes

Data transfer rates particularly depend on the channel coding - see Table 1. The fastest data transfer could be received with CS-4 coding, which is used when radio link with base transceiver station (BTS) is good (high S/N ratio). The most reliable coding is CS-1, but data is transferred much slower.

Using the CS-4 coding it is possible to achieve about 21 kbps data transfer rate. However, the active area will be only 25 % of entire cell area. CS-1 can achieve 9.0 kbps transfer rate, but the active area increases to 95 % since it is applicable with noisy signal. By upgrading the network equipment, there can be an opportunity to automatically determine transmission rate depending on the location of mobile user.

Table 1. GPRS coding schemes.

Coding system	Data rate per time slot, kbps
CS-1	9.05
CS-2	13.4
CS-3	15.6
CS-4	21.4

4.1. Mobility Management States

GPRS has three different states of mobility management - see Fig. 3.
1. *IDLE* state is present when subscriber (MS) is passive (GPRS is not connected). The network does not have any information about the subscriber. To change this state MS should initiate the GPRS connection procedure.
2. *STANDBY* state says that subscriber is active, i.e. is connected to the GPRS service. The network stores all the information about the subscriber and includes MS to the routing table. If MS starts to send data, the status will be changed to *READY*. The GPRS disconnection procedure can be initiated by network or MS and the status of MS will be changed to *IDLE.*
3. *READY* state is activated when subscriber transmits data or is preparing to do this. SGSN may send data to mobile station without paging at any time, the same way as MS can send data to SGSN at any time. If the state timer expires, MS is moved to *STANDBY* state. If the MS initiates detach of GPRS procedure, the state becomes *IDLE.*

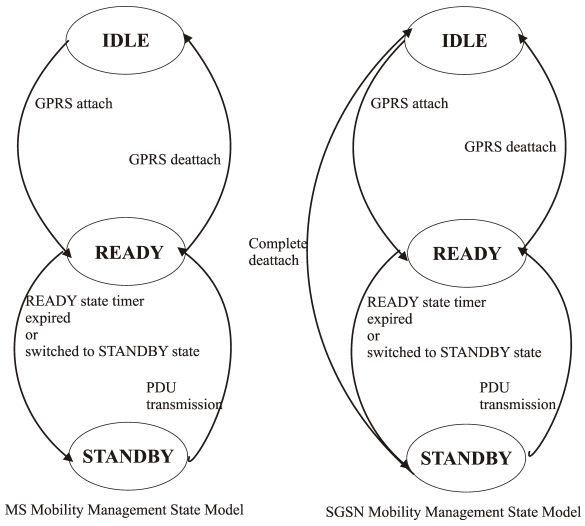

Fig. 3. Mobility management states.

4.2. Packet Data Protocol (PDP)

To initiate the exchange of data, *Packet data protocol* (PDP) must be activated in mobile station, SGSN and GGSN nodes. This procedure is initiated by consumer and can be compared to logging on to an appropriate network. The process is showed in Fig. 4.
1. The user of GPRS network initiates the "logging on" operation by using the existing applications on the mobile station. MS sends the request to the base station to start PDP activation process. When the radio resources are allocated, MS sends the active PDP request to the SGSN. The key information is included in this signaling message: user's static IP address (if given), the APN of external networks (to which an attempt to connect is made), the user identification and other necessary IP configuration information. SGSN accepts the activated PDP request and checks the user's subscription record. This way SGSN checks if request is correct and valid.
2. If this request is valid, SGSN sends another request with sender's APN information to the DNS server.
3. DNS server uses the APN information to identify the IP address of GGSN, which is required for the connection to the external network.
4. SGSN sends the request message to GGSN trying to get in touch and build a tunnel connection.
5. When GGSN confirms this request, the tunnel connection is established. IP address is returned to SGSN, which later is sent to the mobile station.
6. SGSN sends a response message to MS (including IP address).

After these procedures are completed, virtual connection is established between MS and GGSN. The GGSN also has an association between the tunnel and the physical interface to the external network. Now MS can freely transfer data to external networks.

4.3. Packet transmission procedure

In order to start GPRS service, first of all a MS should be connected to GPRS network (i.e. should be in state *STANDBY* or *READY* and the packet data protocol must be activated.

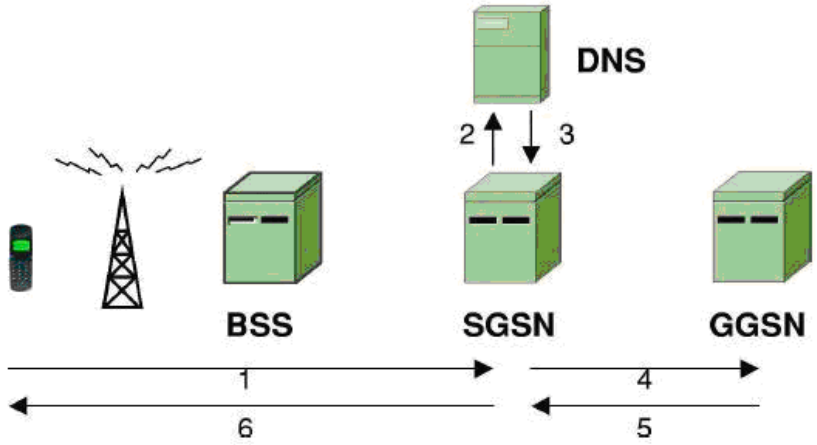

Fig. 4. PDP Context Activation Process

The temporary logical link identity and network service access point identifier identifies the packet data protocol between MS and the SGSN. The tunnel identifier recognizes the packet data protocol between SGSN and GGSN.

4.4. Packet data transmission initiation

When MS wants to transmit data in GRPS network, it sends the request i) on *Packet Random Access Channel* (PRACH) if this logical GPRS channel is established in cell; or ii) *Random Access Channel* (RACH), if PRACH is not established. The packet control unit (PCU) sends a response message with one or several uplink state flags (USFs) (if MS can link several time slots, MS can have different USFs for each separate time slot) and one *temporary flow identifier* (TFI). TFI is the same for all time slots. This message is sent over the radio interface on *Packet Access Grant Channel* (PAGCH) if this logical GPRS channel is configured in the cell or with the *Access Grant Channel* (AGCH) if PAGCH is not implemented [7].

After this procedure one or several uplink time slots are assigned to MS. As soon as the MS receives one of its USF on the corresponding downlink time slot, the MS has to send some data with the TFI on the following radio block of this time slot.

4.5. Paging procedure

If MS is in *STANDBY* state, then only the current routing area is known to the SGSN node. So SGSN should send request message to MS (to start the paging procedure), because otherwise the downlink data transmission would not be possible. The paging procedure is shown in Fig. 5.

1. SGSN receives some downlink data packets dedicated to mobile station, which is now in *STANDBY* state.
2. SGSN sends the base station system GPRS protocol (BSSGP) paging request message. This message contains *Packet Temporary Mobile Subscriber Identity* (P-TMSI), information about PDP routing area and QoS. This BSSGP message initiates the paging procedure.
3. One or several packet control units (this depends on the routing area of cell controlled by one or several PCU) send the request message of location verification (including P-TSMI) to MS. Each message is sent over the radio interface on the *Packet Paging Channel* (PPCH) if this logical GRPS channel is established or on the *Paging Channel* (PCH) if PPCH is not implemented.
4. When the GPRS paging message is confirmed a MS sends the packet channel request on *Packet Random Access Channel* (PRACH) if this logical GPRS channel was configured in the cell or on *Random Access Channel* (RACH) if PRACH was not implemented.
5. PCU returns the immediate assignment packet message (one or several downlink time slots are assigned to MS) with *Time Flow Identity* (TFI). The message is sent over the radio interface on PAGCH if this logical GPRS channel is established in the cell, otherwise on AGCH.
6. MS should respond at least with one valid logical link control (LLC) frame, which will approach as the SGSN paging response message. When the response is received, the MS changes its mobile management state to *READY*.
7. After LLC frame is accepted, the PCU adds it in the global identity of cell. The global identity consists of *Routing Area Code* (RAC) and *Location Area Code* (LAC). Such LLC frame is sent to SGSN and the SGSN accepts this LLC frame as the paging response message.

MS should be in *READY* state after the listed sequence is over. When MS recognizes the assigned TFI in one of its downlink time slots, MS starts packet data transfer.

5. Realization of SCADA system

SCADA system is usually realized in various industries using known commercial technical equipment and software solutions [8]. A simple SCADA system can be created by developing proprietary software and embedded controller driven *Client - Server* system.

First of all, a remote terminal unit which collects data (for example from sensors which measure temperature and send it to server) must be created. RTU is a microcontroller, so assembly board with some connections needs to be made: one connection to connect the modem and the rest for sensors connection. When selecting microcontroller, one should evaluate the quality and price ratio, supported command set and other parameters like speed, memory, programmable flash memory, quantity of I/O ports, timers, etc.

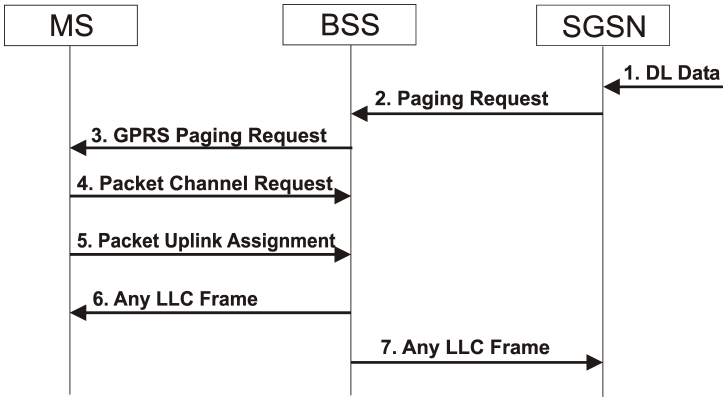

Fig. 5. GPRS paging procedure.

The measurements results should be sent to server over GPRS networks [8]. To send data in GPRS networks, the modem needs to be attached to the RTU board. It is recommended to select the modem which already has the TCP / IP stack protocol, otherwise the protocol needs to be programmed. All GPRS settings are configured in modem using AT commands (depends on modem manufacturer). For realization of data transmission, the socket (combination of IP and port number) should be created.

The last element of SCADA system is the main computer - server, which has the required software that sometimes is called the telemetry system program. To create a simple telemetry system, advanced knowledge in PHP, C++, MySQL, XTML, etc is required. Additionally, several questions, like: i) how many RTU will be maintained; and ii) how many sensors each RTU can have; iii) which structure and coding of packet data should be used as well as other details should be considered.

The main function of telemetry program is to store received data, for example to make history at what time what event was registered and what parameters it had. If the threshold conditions are exceeded, the threshold alarm will be turned on. The threshold alarm can be imagined as a sound, light signal, or, if only particular people must be informed, sms or e-mail should be sent to them. It can be the control command, relayed to remote device, also.

It is possible to think up many SCADA realization forms, with different quantity and types of sensors or threshold alarms. However, the main principles of SCADA system operating and implementation remain the same.

Conclusions

SCADA systems are a vital part of many technological processes that are used in various areas of modern society. These can include such industry segments as energetic (electricity, heating and water supply accounting, water and electricity plants, etc.), production, meteorological data acquisition systems, telecommunications, scientific experiment and other fields. Educational and scientific fields also benefit from the usage of SCADA systems which help conduct the latest researches and experiments, make forecasting, communicate and share knowledge between scientists and universities in the scientific community.

It is shown that the most appropriate medium to use for communication in SCADA systems is GPRS networks due to its reliability, ubiquitous character and pricing. GPRS has many benefits which place it first among all the communication technologies available for usage of SCADA systems, for example GPRS is based on GSM architecture, so no new technologies need to be implemented.

The reader is introduced with SCADA system and GPRS, their main elements and functions are analyzed in this article.

References

1. R. Dennison, A SCADA System Assessment, 2004, Nota Bene Technology. [http://www.nbtinc.com/scada-system-assessment.html], retrieved 2009 03 20.
2. B. Berry. SCADA Tutorial: A Quick, Easy, Comprehensive Guide, v.1.2. DPS Telecom. [www.dsptelecom.com], retrieved 2008 12 02.
3. What is GPRS (General Packet Radio Service)? [http://www.tech-faq.com/gprs-general-packet-radio-service.shtml], retrieved 2009 01 19.
4. J. Eberspächer, H.-J. Vögel, C. Bettstetter, C. Hartmann GSM - Architecture, Protocols and Services, Wiley, 2009, 338 p.
5. An O2 White Paper: GPRS: How all Works. [http://www.o2.co.uk/assets/O2HybridNav/Static-files/PDFs/ GPRsHowAllWorks.pdf], retrieved 2009 01 09.
6. E. Seurre, P. Savelli, P.-J. Pietri , GPRS for Mobile Internet, Artech House Publishers, 2003, 438 p.
7. S. Geoff, L. Thoren. GPRS Networks. England, 2003, p. 100-113.
8. D. Baley, E. Wright. Practical SCADA for Industry. - Great Britain, Newnes, IDC Technologies, 2003, p. 1-36, p. 72-80.