GPRS
Technology & Applications
Implementation of Telecontrol Applications over GPRS Networks

This article introduces GPRS (General Packet Radio Service) technology and examines its applicability to the sphere of telecontrol communications in an electric utility. In order to do so we will perform an analysis of the technology and its possibilities, telecontrol protocols, and give specific examples of why traditional telecontrol applications which function correctly over point-to-point serial links require a reformulation which optimises their function over a communications technology such as GPRS. It will also be analyzed whether this technology fulfils the reliability requirements expected by utility communications.

Given that GPRS operator networks are public, the implications of this fact are examined from the utility’s point of view, and finally we list the most important aspects to be considered in order to perform a successful implementation of a telecontrol system over GPRS.

Companies in the electric sector have a multitude of SCADA Telecontrol systems which operate with protocols aimed at serial ports, for example IEC 60870-5-101, DNP3... Historically, communication with remote sites has been performed using the electric company’s private communications channels, such as PDH, VHF and microwave radio or others. This option was the only one available capable of covering the communication requirements for the provision of service.

In the present day, companies are under increasing pressure to reduce infrastructure operating costs, but at the same time maintain (or increase) the availability and reliability of their communications. As such, new methods of communication are being explored to allow them to do so. A clear alternative is the use of public communications networks, using a service provided by an operator. One option which has been used for some time is data calls, either over a fixed or mobile (GSM) network.

In recent years, with the development and progressive implementation of packet switching technologies over mobile networks (GPRS/UMTS/EDGE), a new range of possibilities has opened up which may make them viable for telecontrol applications. On the one hand, a TCP/IP-based service is offered, which guarantees the reception of traffic and the “always online” nature of this type of service. Further, charges based on exchanged traffic volume, as opposed to circuit switching connections which are charged by connection time, may be a very attractive feature for utilities. Only the traffic actually exchanged is paid for.

Nevertheless, each of the telecontrol protocols which were once designed for implementation using serial ports have their peculiarities which make direct use over a TCP/IP network, with the inherent latency of a GPRS network, problematic and even unviable. There are a number of determining factors which must be considered for telecontrol communications to be rolled out appropriately and reliably. On the other hand, the main source of reluctance to using GPRS networks on the part of electric companies lies in the difficulty in monitoring and verifying the level of service provision promised by the mobile services operator, given that this comprises an aspect which the electric company does not possess a sufficient level of control over or means to verify.

This article summarises all of the aspects which must be considered in order to successfully and reliably establish a telecontrol application over GPRS, and details the parameters and methods which must be taken into account by the electric company to control the quality of service provided by the operator.

Serial telecontrol protocols and their peculiarities
Telecontrol protocols used over a serial port communication interface were initially designed for

Aitor Arzuaga Munsuri graduated at the ETSIT Bilbao in 1999. He began his career as a grantee at Hewlett Packard, then moved to Ericsson. In 2002 he joined uSysCom, a branch of ZIV, and designed hardware for utility communications equipment. He is an active member of Cigé groups, a representative of the Spanish committee in IEC TC57WG10 and a member of IEEE. He has many articles about communications for industrial applications. Since mid-2009, Aitor is head of R&D activities at ZIV.

Jose Miguel Arzuaga Canals or Txetxu for friends obtained in 1998 his Telecommunication Eng. degree. He started his carrier in Vodafone, Spain, with positions in the IT area. In 2000 he started a new job in an Ericsson unit, whose goal was to make machines talk. At present, Txetxu is the general manager of uSysCom, a spin-off company in ZIV, uSysCom designs and manufactures telecom equipment for the Electrical Utilities.
GPRS technology has reached sufficient levels of maturity and reliability.

Transmission methods characterized by the following properties:
- Negligible latency in relation to the bit speed used (<100 kbps), as is the case with a copper wire a few metres in length or optical fibre up to hundreds of metres in length. In both mediums, the signals travel at a fraction of the speed of light.
- Strict timing requirements
- Very low Bit Error Rate (BER), which can be estimated to be less than \(1 \times 10^{-10}\)
- A purely physical medium with data recovery or error correction mechanisms (there is no link level)

- Unlimited total traffic volume or usage rate of the serial link, not relevant
- By means of a simple analysis we can conclude that a GPRS communications channel has characteristics very different to those mentioned above:
  - Latency can be considerable, reaching values from 200 ms per link (typical for UMTS), 500-700 ms (typical for GPRS) and up to several seconds (GPRS with low coverage and a traffic-saturated network)
  - Although the BER is very high in radio traffic, the modulations employed are robust, and coding and error correction ensure that traffic sent to the application is error-free. However, all of these errors manifest themselves as variance in link latency. Sending delay depends on radio transmission conditions at any specific time
  - Lost frames are common. However, the TCP/IP protocol takes care of recovering them in the appropriate order after a few seconds. There are transport, network and link levels below application communication
  - Traffic cost is calculated by volume. The total amount of traffic is important.

Some telecontrol protocols which are commonly used in telecontrol applications and which are appropriate for use over a GPRS connection include IEC 60870-5-101, DNP3, GESTEL, SAP20, PID1... In general any protocol which fulfils the following criteria can be adjusted to transmission over GPRS:
- Frame format correctly defined by characters or binary sequences at the beginning and end of the frame, avoiding ambiguities (predefined escape sequences)
- Predetermined maximum and minimum frame lengths, and where possible not too long as this impacts negatively on latency. Satisfactory results have been obtained with a value of 256 bytes
- Error detection mechanism in the protocol frame itself (CRC or similar) which allows for validation of the integrity of the protocol frame at both ends

Example of a telecontrol application over GPRS

In a typical telecontrol application which we will take as an example, there is a serial connection between a Control Center, generally located in an office, and a telecontrol RTU located in a remote installation. The serial Control Center – RTU connection is realized by means of a radio communications channel, microwave links (private channels) or by satellite and telephone networks (third-party channels). In the proposed solution over GPRS shown in Figure 1, the serial link is replaced by a TCP connection over GPRS.

In order to implement a telecontrol solution over GPRS it is necessary to add encapsulators to perform the following functions:

1. Telecontrol application over GPRS
**GPRS can be applied in telecontrol applications, either as a backup for private communications channels or as a main communications technology.**

- Establish an end-to-end TCP connection over GPRS and maintain the same using connection management mechanisms (keep-alive or similar)
- Analyze protocol frames received by the serial port, verify their integrity and IP encapsulation, broadcast over a LAN or GPRS network
- Manage the sending of frames over GPRS, filter unnecessary protocol traffic (for example, QuickCheck messages or similar), in order to minimize the cost of traffic sent (*only relevant traffic is sent over the costly GPRS link*)
- Manage the sequence of protocol messages so that lost protocol messages which are subsequently retransmitted by the TCP protocol are removed, given that this tends to produce dropped connections in Control Centers and Remote installations (Figure 2)

As can be observed in Figure 2, problems can arise in telecontrol applications over GPRS which use protocols initially designed for application on serial ports if all lost messages are allowed to be recovered by the TCP protocol. If the recovery occurs after the Control Center has retransmitted the original protocol message, it will receive two answers, one of which will be out of sequence. As a result, depending on the configuration of the control center, this will cause the link to be reset and recovered.

In practice, this makes the GPRS link unusable for a telecontrol application under low coverage conditions because the protocol link is dropped and recovered constantly. By implementing sequence control on the end encapsulators, the problem is avoided and the link is reliable, without the need to reconfigure the protocol time parameters of the Control Center (which may not even be viable or desirable).

It is also extremely important to adjust all of the application timeouts in telecontrol applications to the new transmission technology. The link latency increases in the order of seconds, and it is therefore essential to increase time values accordingly. For example, in some implemented systems, application timeouts of around 1 second have been increased to 10 seconds, obtaining good results.

**GPRS networks and their applications**

The GPRS system (General Packet Radio Service) is an additional mobile data service offered over GSM networks. GPRS is a packet switching service, directed at the use of TCP/IP applications. As such, this system is suitable for applications such as Internet navigation or file exchange.

The GPRS service is offered on a number of GSM frequency bands (800, 900, 1800, 1900 MHz) as a complimentary service, with practically worldwide coverage (except for Japan and Korea).

The GPRS service allows for packet mode data transmission speeds from 9 to 40kbps (uplink) and 9 to 80kbps (downlink). This transmission technology is therefore asymmetric in terms of data speed. There are evolved versions of the technology such as EDGE (Enhanced Data rate for GSM Evolution) which allow higher transfer rates (up to 236 K bps downlink and 60 kbps uplink), and these are available in many countries.

GPRS technology therefore presents multiple applications in the world of Telecontrol, given its reliability and high coverage. Nevertheless, there are some aspects of GPRS networks that need to be considered.

---

**2 Sequence control of protocol messages in a GPRS encapsulator**

<table>
<thead>
<tr>
<th>Control Center</th>
<th>RTU</th>
<th>Control Center</th>
<th>RTU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request 1</td>
<td></td>
<td>Request 1</td>
<td></td>
</tr>
<tr>
<td>Response OK</td>
<td></td>
<td>Response 1 is lost in transit</td>
<td></td>
</tr>
<tr>
<td>Incorrect Response received, Error!</td>
<td></td>
<td></td>
<td>The device detects the out-of-sequence Response and filters it</td>
</tr>
<tr>
<td>Link Reset Request</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

GPRS connection without sequence control

GPRS connection with sequence control
which must be considered in order to achieve effective implementations:

- **Latency** is extremely high in GPRS networks, in the order of 500 ms to 2s per GPRS link, is not deterministic and also has high variance, even for successive packets. This must be taken into account for telecontrol applications.

- The GPRS network is a radio network, and as a result of varying transmission conditions and their variation over time, packet losses occur. If the TCP/IP suite of protocols is used, packets are subsequently recovered and delivered to the application in order. This leads to retransmissions and a considerable increase in traffic latency.

- **Traffic cost.** Traffic is charged per byte transmitted, or by large blocks of traffic bought from the operator. This leads to a change with respect to traditional wired networks, where traffic is free once the infrastructure has been rolled out.

Some network operators offer their customers the possibility of obtaining a private IP domain (GPRS intranet), meaning they obtain a subnet of private IP addresses, isolated from the internet and other GPRS users, and accessible only from other points in the private IP subnet. Figure 3 shows some telecontrol applications and others of interest to electric companies which can be implemented over a GPRS network.

**Public communications channels' usage**

There is a certain degree of reluctance among companies in the electric sector towards using public communications infrastructures for the provision of telecontrol services. This is due to the existence of a series of factors which used to make this strategy ill-advised, such as:

- Reduced availability and reliability of public communications solutions compared to private ones
- Increased security of using a private network which is completely closed off to the outside world
- Strategic issues (autonomy in service provision) and organizational ones with respect to the electric utility

In recent years factors have also appeared which would seem to favor the use of operator or public communications networks:

- Constant (growing) pressure on electric utilities to reduce...
operational and maintenance costs.

- Solution scalability. The number of connections can be increased by contracting them from the operator (or contracting another operator).
- Independence from technology employed, given that the infrastructure is owned by the operator and only its use is contracted.
- Improvement in geographic coverage of public networks. It is increasing in all countries and an increasing proportion of inhabited territory is covered.
- Progressive improvement in communications service quality provided.

If we take all of these factors into account, we can draw up a series of general recommendations which can make the transition to using GPRS networks for telecontrol applications simpler and less traumatic for a utility company. We list these arguments below:

- If using an external communications network for telecontrol services is considered too great a risk, GPRS networks can also be used as an alternative communications channel together with private communications networks (for example, private radio links and GPRS as a backup). Using this approach, the utility gets improved redundancy and enhanced reliability with a limited investment and small operation costs.
- Performing a preliminary coverage study for planned sites, with each of the different GPRS operators present in the country, in order to avoid low signal strength problems or the inability to establish communications in the implementation phase. This will provide information on what sites are viable out of the total number required, and as such, assess the viability of GPRS technology for service provision.
- Use, as far as possible, operator redundancy policies, by using devices which allow communications to be established through two operators (double SIM card). In this way, it is possible to establish communications with a GPRS operator, and in the event that it fails, the GPRS device switches automatically to the second operator, allowing communications to be re-established. Preliminary experience with this redundancy functionality in Spain demonstrates an increase in system availability to over 98%, compared to 90% with a single operator.
- It is important to ensure the security and privacy of telecontrol information. Two levels of security should be established:
  - The first consists in contracting the use of an Intranet or VPN with the GPRS operators, so that the range of IP addresses assigned to the telecontrol applications are private and therefore inaccessible from any point outside of the electric company IP network.
  - The second level of security entails the use of IPSec or SSL/TLS tunnels with certificates between the remote devices and the utility company’s external access firewall, as can be seen in Figure 4. This ensures a level of total privacy, in such a way that not even the GPRS operator itself can access the information sent, at the cost of increased complexity in system configuration, implementation and management.

 Requires a review & analysis of a number of aspects:
- (protocol, configurations, network architectures, terminal elements and control centers) in order to ensure that the telecontrol system is capable of functioning reliably, effectively and efficiently, and it can complement existing systems to improve reliability.

4 Telecontrol application over GPRS with TLS security

GPRS main disadvantage lies in the fact that coverage is reduced to inhabited areas.