The communication unit for remote data acquisition via the Internet

PETR MLYNEK, MARTIN KOUTNY, JIRI MISUREC
Department of Telecommunications, Faculty of Electrical Engineering and Communication,
Brno University of Technology, Purkynova 118, 612 00 Brno, CZECH REPUBLIC

Abstract: The most widely used networks for data communication are TCP/IP networks. One of the application areas is the remote data acquisition in power engineering, where the consumption of electric power is read in so-called continual metering. Electrometers can be connected to the TCP/IP network by means of the communication unit. Thanks to the communication unit, remote acquisition of power consumption data is enabled. This article focuses on the connection and the methods of testing of communication unit in an experimental network. The article also deals with the design of the authentication, secure data transmission, and transmission block integrity.

Key-Words: communication unit, remote data acquisition, Internet, measuring device, electrometer, PQ monitor, authentication, transmission block

1 Introduction

The Internet is now the widest network used for data communication. The tendency to make maximum use of it for data transmission from various devices requires creating appropriate communication units which allow connecting various devices to the Internet, such as electrometer. An electrometer can be connected to the Internet by means of a communication unit, enabling remote acquisition of data on power consumption.

An advantage of remote data acquisition is the possibility of frequent readings without physical presence at the electrometers. Data transmission over the Internet can be the subject of various attacks, which is a disadvantage. For this reason it is necessary to design and include authentication tools in the communication unit and have the possibility of encrypted data transmission.

Communication for network control, monitoring and power consumption metering is mainly running on communication channels based on the RS-232 standard. The construction of new communication channels is expensive and impractical and thus current communication channels will be used, in our case the Internet. For this reason, the communication unit is designed as an RS232/Ethernet transducer and vice versa.

The communication unit enables connecting single-purpose devices for measuring electric quantities of the power network to the Internet via the TCP/IP protocol. Information from these measuring devices is transmitted to a telemetric acquisition system.

The communication unit is built on the basis of the RMC3700 module with a Rabbit3000 microprocessor. The Rabbit3000 microprocessor operates at a frequency of 22.1 MHz, and has sufficient power reserve for implementing also more complicated security algorithms. Currently, the module software is being designed, with the 512KB Flash memory configuration being considered for the program and 512KB SRAM for the data. The module implements the transducer from interface RS232 to Ethernet. [1]

2 Communication string

Fig. 1 shows the communication string of the system of telemetric data acquisition. The station initializes communication via the encryptor, which is then connected to the appropriate cryptography module of the communication unit. After successful mutual authentication, communication can start between the acquisition station and the measuring device.

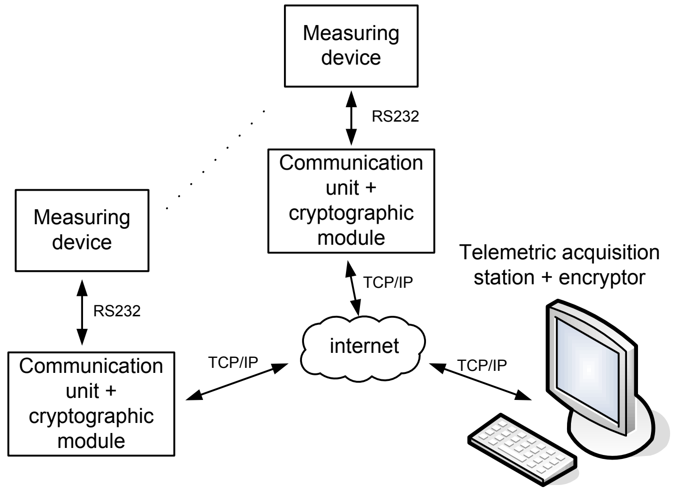
Measuring device
RS232
Communication unit + cryptographic module
Measuring device
RS232
Communication unit + cryptographic module
TCP/IP
TCP/IP
internet
TCP/IP
Telemetric acquisition station + encryptor

Fig. 1: Communication string

The telemetric acquisition station represents the central point of the network, assuring data collection in its sub-domain. The encryptor is implemented in the station and ensures cryptographic operations in the telemetric acquisition station. Its task is dual authentication while connecting to the cryptographic module, i.e. decrypting the data stream running from the metering facility or encrypting the data stream running towards the metering facility.

The communication unit contains an RCM3700 module. The RCM3700 module is a cryptographic module assuring cryptographic operations connected with the protection of data transmission. Together with the encryptor it implements authentication and secure transmission of the data measured.

3 Communication unit testing using a measuring device

Testing the functionality of the communication unit of remote data acquisition was realized with the PQ monitor MEg33 and the CU-E21 communication module of electrometer.

3.1 PQ monitor MEg33

The PQ monitor is designed for metering voltage quality parameters according to the EN 50160 Standard. More detailed information about the PQ monitor MEg 33 can be found in [2]. The communication unit is connected directly to the PQ monitor, because it contains the RS-232 interface. The PQ-monitor software was not primarily designed for remote data acquisition via the TCP/IP protocol and therefore a mediator was used, which enabled the simulation of serial port. This virtual port was then adjusted, as if it was physically present. Incoming requirements on this port were sent by the TCP protocol to a preconfigured IP address of the unit. The simulation environment is shown in the following figure:

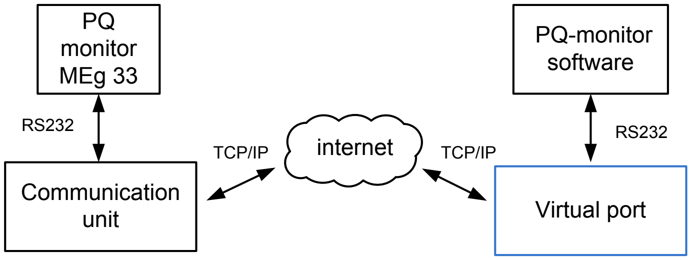

Fig. 2: Simulation environment

3.2 Communication module CU-E21

The electrometer ZMD 310 [3] does not enable communication over the RS-232 interface, but via the communication module CU-E21 it is possible. Module CU-E21 [4] contains the RS-232 serial interface. CU-E21 represents the interface between our communication unit and the electrometer.

In our experimental network, data exchange between the electrometer and the telemetric acquisition station is implemented by the Energy Data Collection (EDC) program [5]. This program provides its services in cooperation with the iMEGA meter2cash and iMEGA Device Driver modules [5]. The task of iMEGA meter2cash is to establish connection with the electrometer and then to share this connection via a virtual serial port in the Windows system. Via the iMEGA Device Driver the virtual port is used to provide communication between the meter2cash program and the virtual serial port. The simulation environment is shown in the following figure:

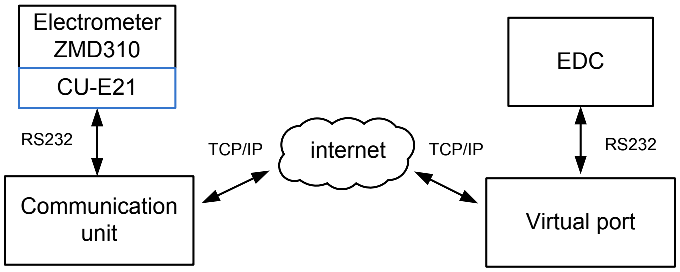

Fig. 3: Simulation environment

4 Model of authentication

Communication between the communication unit and the acquisition station is divided into authentication and the data transmission itself. The communication process is based on the principle of symmetric cryptography, specifically on the block cipher with ECB and CBC modes and AES algorithm. The authentication algorithms are based on the ECB mode. The data transfer is based on the CBC mode.

A precondition for the functioning of authentication is that the value of distribution key, DK, is known to both sides. The distribution key is used only in authentication transmissions. Using all the time one and the same key for secure data transmission entails the risk of potential cryptanalytical attack on the basis of periodization. For this reason, the key must be changed from time to time. [6]

More detailed information about the choice of cryptography can be found in the literature [7]. Fig. 4 illustrates the design of authentication and establishment of keys for transmission.

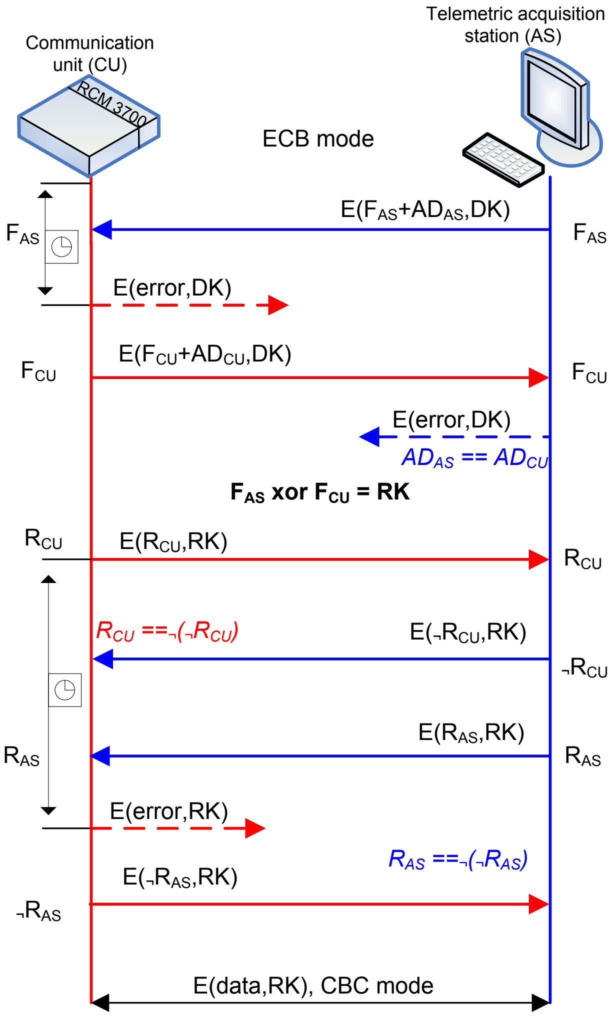

Fig. 4: Model of authentication

Where:

DK is the distribution key for *CU;*
R_{CU}, R_{AS}, F_{CU}, F_{AS} are random numbers;
$\neg R_{AS}$, $\neg R_{CU}$ are negated R_{AS} and R_{CU};
AD_{AS}, AD_{CU} are the addresses of *AS* and *CU;*

Description of authentication [7]:

1) When establishing the connection, *AS* generates a random number F_{AS}. This number F_{AS} together with the address of *AS* is encrypted with a common distribution key *DK* for a given cryptographic module of *CU*. The resulting cryptogram $E(F_{AS}+AD_{AS},DK)$ is then sent to the respective cryptographic module.

2) The cryptographic module of *CU* waits for a definite period of time to receive the cryptogram. If the cryptogram does not arrive, the cryptographic module

sends an error message to the telemetric acquisition station *AC* and *CU* returns to the initial state. When the unit has registered an authentication attempt within a defined period of time, it generates a random number F_{CU}. This number F_{CU} together with the address of *CU* is then encrypted with the distribution key. The resulting cryptogram $E\,(F_{CU} + AD_{CU}, DK)$ is sent to the telemetric acquisition station *AS*.

3) At both ends, the random numbers and addresses received are decrypted by the distribution key. After that, the addresses are checked. If the sender address and the receiver address are different, then the exclusive *or* operation with the two random numbers is performed. The result is a key $RK = F_{AS} \oplus F_{CU}$.

4) The cryptographic module of *CU* generates a random number R_{CU} and encrypts it with the key *RK*. The resulting cryptogram $E\,(R_{CU}, RK)$ is sent to the telemetric acquisition station *AS.* The cryptographic module starts the timer and waits for a specific period of time for the response from *AS*. The telemetric acquisition station *AS* receives the cryptogram $E(R_{CU}, RK)$, decrypts it and obtains a number R_{CU}. It negates this number, encrypts it with the key *RK* and sends it back as a cryptogram $E\,(\neg R_{CU}, RK)$. The cryptographic module receives the cryptogram $E\,(\neg R_{CU}, RK)$, decrypts it, and compares $\neg R_{CU}$ with R_{CU}. Then it decides on the success of authenticating the telemetric acquisition station, which brings the process of authenticating the *AS* to an end.

5) The telemetric acquisition station *AS* generates a random number R_{AS}, encrypts it with the key *RK* and sends the cryptogram $E\,(R_{AS}, RK)$ to the cryptographic module of *CU*. If the cryptogram comes within a definite period of time, it is decrypted by the cryptographic module and a number R_{AS} is obtained. This number is negated and then, encrypted with the key *RK,* sent in a cryptogram $E\,(\neg R_{AS}, RK)$ back to the telemetric acquisition station *AS*. The telemetric acquisition station *AS* decrypts the cryptogram and compares the two numbers, R_{AS} and $\neg R_{AS}$. If the numbers are identical, the process of authenticating the cryptographic module of *CU* is completed.

6) The establishment of authentication process is followed by the transmission of encrypted data using the CBC mode and the computed key *RK,* which thus becomes different for each connection.

The verification of addresses is designed for the protection against reflection attack. An attacker can catch the first cryptogram from *AS* and send it back to the *AS* as a first cryptogram from *CU*. *AS* will calculate the key *RK* = 0, because the exclusive *or* operation with two identical numbers is zero.

Time limitations on the communication unit side are designed for the case that the packet gets lost or has a major delay in the network.

5 Transmission block

Fig. 6 shows the format of an encrypted message. The CBC mode is used for the process of secure data transmission. It is therefore necessary to fill the data with padding bits for the sake of preserving the required size of data block. Since we use PAD bits, it is also necessary to know for decrypting the message how many bits from the block are taken up by the message and how many bits are used for filling. For this reason, 16 bits of the message have been reserved for information about the block length LEN. Another 16 bits have been reserved for message check sum CRC, which together with the CBC mode guarantees data integrity. The application of initialization vector follows from the principle of CBC mode. This vector will be generated for each transmission randomly in order to assure a dissimilarity of the messages transmitted.

Communication with the PQ monitor works on the instruction-response principle. In an experimental network testing procedure it was established that the PQ monitor software divides instructions into several blocks. These instructions are encrypted and sent to the communication unit over Ethernet.

These blocks are received by the communication unit, but these blocks came in one stream. These blocks are decrypted by the communication unit and the check sum is calculated. The check sum is not correct, because it was calculated from several blocks (see Fig.5).

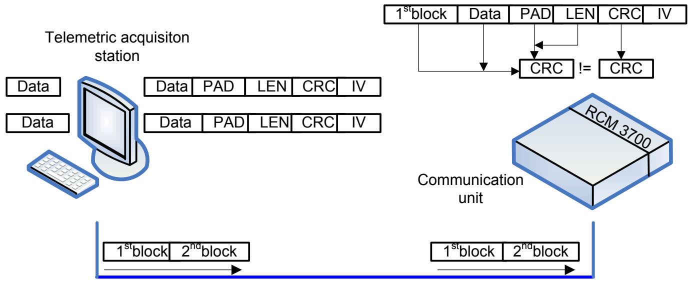

Fig. 5: CRC calculation

For this reason a new transmission block was designed. The new block contains, in addition, the total length of the block. The total length is calculated without an initialization vector. In the case of an intentional change of the total length, the attacker is not able to ensure the corresponding check sum for this block.

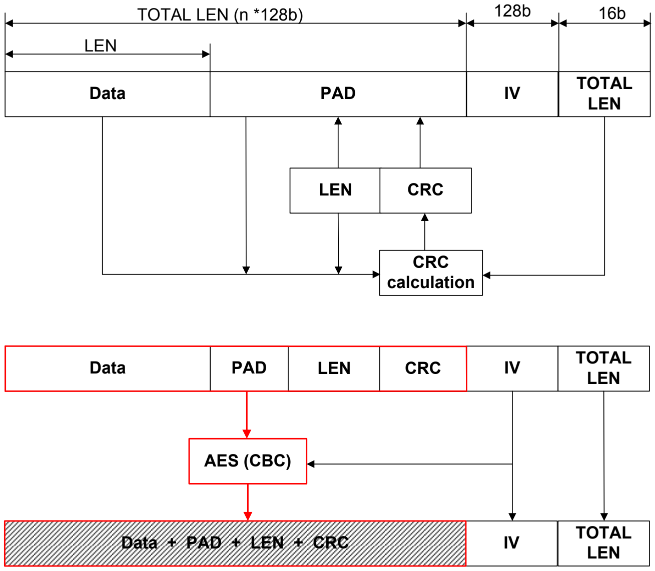

Fig. 6: Transmission block

An algorithm is designed on the communication unit side (see Fig. 7) that reads the total length value from the data received. This value is compared with the real length of received data. If the values are the same, only one block was sent. If the values are different, then the total length of next block was read. If the sum of the two total lengths is the same as the real length of received data, two blocks were sent. If not, the algorithm will continue running.

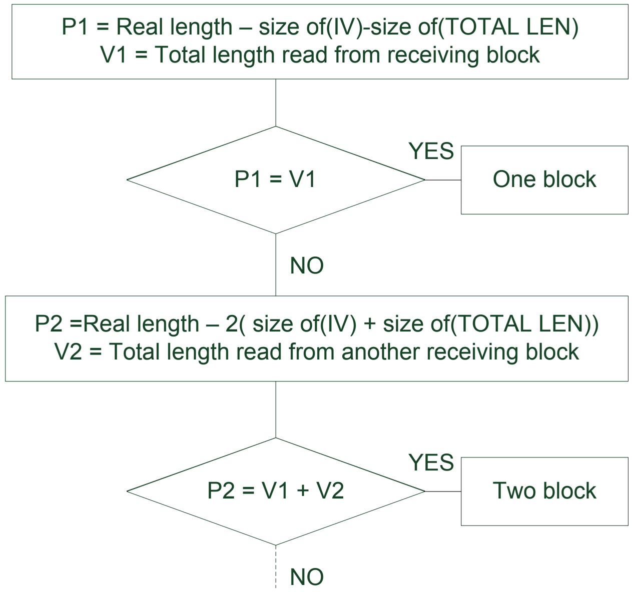
P1 = Real length – size of(IV)-size of(TOTAL LEN)
V1 = Total length read from receiving block
P1 = V1
YES
One block
NO
P2 =Real length – 2(size of(IV) + size of(TOTAL LEN))
V2 = Total length read from another receiving block
P2 = V1 + V2
YES
Two block
NO

Fig. 7: Flow diagram

6 Conclusion

Great accessibility of Internet offers a lot of benefits, but also brings many security risks. Great accessibility predestinates it for data transmissions and remote data acquisition from measuring equipment.

The communication unit serves to secure data transmission between energetic devices and the power network operator. The communication unit contains a serial interface, which is included in most energetic devices for local data acquisition. This serial interface is converted to the Ethernet in the unit. This transducer enables connection to the Internet and remote data acquisition.

The paper describes two possible methods of testing the functionality of communication unit. In one method, the PQ monitor MEg 33 is used, which is designed for metering the voltage quality parameters. In the other method, the CU-E21 communication module of electrometer is used.

Data transmission over the Internet can be the subject of various attacks and therefore secure authentication and secure data transmission are described in this article. The new transmission block, which ensures a secure and reliable data transmission, is described too.

The paper suggests a possible implementation of a simple authentication algorithm. Authentication works on the principle of two secret random numbers, which are exchanged in the authentication mechanisms. From these random numbers the encryption key for data transmission is derived.

7 Acknowledgement

The paper was written within the Czech Academy of Sciences project No. 1ET 110530523.

References:

[1] Rabbit Semiconductor Inc.: *RabbitCore RCM3700: User's Manual*. 2005. 166p.

[2] MEgA Měřicí Energetické Aparáty: *PQ monitor: MEg30, MEg31, MEg32 a MEg33*. 2006. Online: <http://e-mega.cz/doc/pqmonitor_mail.pdf>.

[3] Landis + Gyr: *ZMD310AT/CT - Technical data*. Online: <www.landisgyr.eu/files/pdf2/LandisGyr_ZXD300ATCT_TechData_EN1.pdf>.

[4] Landis + Gyr: *Communication unit CU-E20, E21, E22 - Technical data*. Online: <www.landisgyr.eu/files/pdf2/7102000320_en1.pdf>.

[5] Landis + Gyr: *Central station DGC300 - User manual*.

[6] MOLLIN, Richard A. *An introduction to cryptography.* 2007. 413 p. ISBN 1-58488-618-8.

[7] KOUTNY, M. *Design of secure communications for measuring equipment networks*. In 8-th International Conference - Research in Telecommunication Technology RTT - 2007. 1. Zilina, Slovakia, ZILINSKÁ UNIVERZITA. 2007. p. 1 - 4. ISBN 978-80-8070-735-4.