Grzegorz LENTKA[1], Sławomir TYBORCZYK[1]

Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics,
Department of Metrology and Optoelectronics (1)

doi:10.15199/48.2016.10.60

Distributed measurement system with data transmission secured using XXTEA algorithm

***Abstract**. The paper deals with wireless data transmission security in the distributed measurement and control system. An overview of cryptographic algorithms was presented paying special attention to the algorithm dedicated to units with low processing power, which is important due to minimization of energy consumption. Measurement modules equipped with simple microcontrollers send data wirelessly to the central unit. The transmission was secured using modified XXTEA algorithm assuring low requirements for resource usage.*

***Streszczenie.** Artykuł dotyczy bezpieczeństwa bezprzewodowej transmisji danych w rozproszonym systemie pomiarowo-sterującym. Dokonano przeglądu algorytmów szyfrowania ze szczególnym uwzględnieniem tych dedykowanych do jednostek o niewielkiej mocy obliczeniowej. Moduły pomiarowe oparte na prostych mikrokontrolerach przesyłają do centrali systemu dane zabezpieczone zmodyfikowanym algorytmem XXTEA o niskich wymaganiach sprzętowych. (**Rozproszony system pomiarowo-sterujący z transmisją danych zabezpieczoną algorytmem XXTEA**).*

Keywords: distributed measurement systems, secure data transmission, XXTEA cryptographic algorithm.
Słowa kluczowe: rozproszone systemy pomiarowo-sterujące, bezpieczna transmisja danych, algorytm kryptograficzny XXTEA.

Introduction

Measurement and control systems using wireless communication have an increasing importance for the industry as well as for the everyday live. The use of radio frequency for communication and remote control seems especially useful in some specific cases: when the object under control/measurement is moving (e.g. car), the object is far away from the user (meteo probes), the object is located in the place difficult to reach or the wiring costs are not acceptable. Generally, taking into account transmission medium, such systems can be divided into three main categories [1]: cellular phone network transmission; selected radio channels transmission (ISM band); infrared link transmission.

Continuous industrial development and a strong trend towards process automation cause a growing need for development of devices allowing to monitor selected environmental parameters and to control actuators. Usually, such devices have to fulfil given requirements specific to the work conditions, like immunity to electromagnetic disturbance and tolerance to weather conditions, remote access or limited physical dimensions. This paper presents the prototype of the modular measurement and control system with GSM based remote access. The main criteria taken into account during system design were: data transmission security, remote access control, modularity, universality, reliability and energy efficiency.

The plurality of cryptographic solutions, assuring the secure remote access and safe wireless data transmission, allows mainly to select and implement an adequate encryption/decryption algorithm, taking into account the available software and hardware resources. In the case of devices powered by a battery or using energy harvesting solutions, it is necessary to consider the energetic effort of encryption/decryption operations, usually, the ciphering time should be as short as possible.

The proposed system architecture

The block diagram of the proposed distributed measurement and control system with GSM communication is presented in Fig. 1. The proposed use of GSM communication allows achieving high mobility and flexibility of the system location (limited only by GSM network range) while assuring high security remote access measurement.

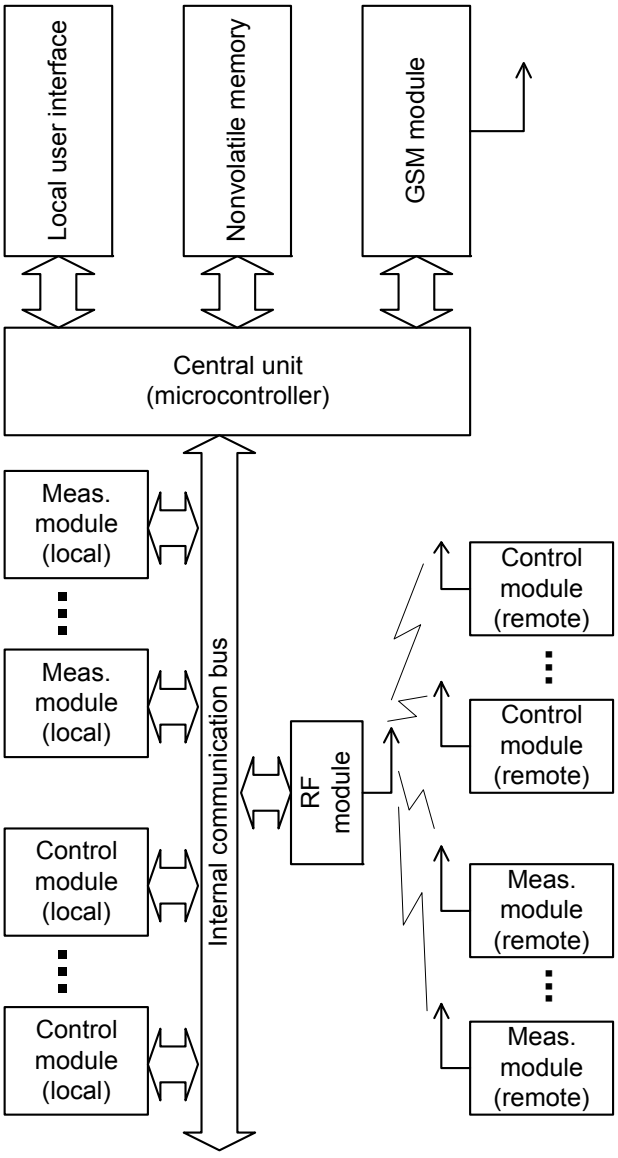

Fig.1. Block diagram of the proposed distributed measurement and control system

GSM module is one of the main parts of the system and assures wireless duplex communication channel between the user and the system. It is assumed that the user can achieve remote access to the system. This means the possibility of sending commands and queries using short text messages (SMS). The commands define what operations the system is able to perform and the queries make it possible to obtain parameters of the system or its components using SMS responses. There is also the possibility of sending automatic text messages informing the user about defined events (alerts).

Microcontroller together with the peripheral blocks, is the main part of the system. The most important tasks of the microcontroller are the communication with GSM modem, the analysis and processing of incoming text messages, the execution of the user commands and queries as well as the preparation of a response message. The microcontroller communicates with other system blocks (measurement and control modules, user interface, nonvolatile memory) via different serial digital interfaces (I^2C, SPI, QSPI).

Because the system can be easily expanded, two types of the expansions modules were designed: measurement modules and control modules, each of them can be connected with the central unit locally (using wires) or remotely (wirelessly). The measurement modules are responsible for determining selected environmental parameters with the aid of the dedicated sensors. The control modules work as output devices; they make driving selected instruments possible with the help of the user messages or in an automated way. In both cases, the microcontroller manages modules activity and makes decisions concerning the measurement (or control) data destination (saving to the nonvolatile memory, response message to the user, etc.). The example view of a simple remote measurement module is presented in Fig.2

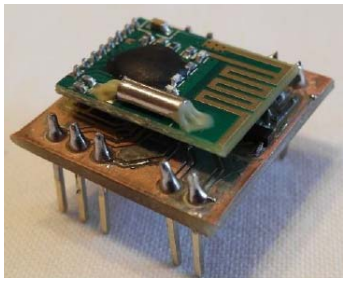

Fig.2. Exemplary prototype of a remote measurement module

The local user interface block allows for a system management when the user has physical access to the central unit or when the GSM access is not possible; or for defining the first GSM terminal identifier authorized to remotely administrate the system. The local user interface block enables to control basic system parameters, check the presence of control and measurement modules, GSM connection status and access other useful information.

Nonvolatile memory is a main data storage and is used for keeping information connected with general system functionality. It is the place for storing configuration settings, acquired measurement data, incoming and outgoing text messages, authorized user phone numbers and other necessary information. The memory can be also used for registration and time stamping of asynchronous external and internal events, like system errors and malfunctions, GSM network unavailability, missed remote user authorisation or the violation of the limits of the measured and monitored parameters.

The power supply block (not shown in Fig. 1) is responsible for supplying correct supply voltages to all system blocks as well as for the voltage level conversion when it is necessary. The main requirement for this block is energy conversion efficiency and a possibly wide input voltage.

Encryption algorithms used in the distributed control and measurement systems

The described modular measurement and control system, due to the GSM communication usage as well as the presence of autonomous measurement and control modules with radio communication, can be counted in the category of distributed measurement and control systems with wireless access [2]. The cryptographic methods and algorithms commonly used in low-power, energy-efficient systems and distributed sensor networks can be divided into three subclasses [3]: hash function cryptography; public key cryptography (asymmetric); private key cryptography (symmetric).

Hash functions are very important components of most contemporary cryptographic systems. They are mainly used for authentication of the user of the distributed system and the authentication of transmitted data (digital signature, data integrity). The hash functions usage is based on a unidirectional feature of the function: it is easy to calculate the function value taking the given argument but there is only a very small chance to find this argument having the function's value (the function is non-invertible). „Very small chance" means, that the calculation complexity of known algorithms of reverse calculation is too high to be physically executed. Input set x with known length is transformed into output set (with defined, usually smaller, length) called hash. The hash function should be, first of all, strongly collision-free, which means, it should be very difficult to find two different inputs x_1 and x_2 giving the same values (hashes) $f(x_1)=f(x_2)$. The hash function security depends on its non-invertibility, and also the change of a single bit in the input should cause the change of approximately the half of output bits (a so-called avalanche effect) [3-5]. There are many hash function algorithms but the following can be incorporated into the most popular in distributed measurement and control systems: SHA family (Secure Hash Algorithm), MD (MessageDigest), RIPEMD, Haval or Whirlpool.

In asymmetric (public key) cryptography algorithms, the data sender encrypts the message using selected algorithm and a public key of the addressee (known). In order to decrypt the message, the receiving side must use a private key (that should be kept secret). The asymmetric cryptography, similarly to hash function cryptography, uses unidirectional functions. Nowadays, there is plenty of popular asymmetric algorithms, like RSA, ElGamal or methods based on elliptic curves. These algorithms are based mainly on four mathematical operations: multiplication, big integer numbers factorisation, modulo exponentiation and discrete logarithms calculation in finite fields [4, 5]. The above mentioned algorithms are seldom used in the distributed measurement and control systems mainly due to long execution time and difficult implementation. Following this fact, in the embedded systems, when there is a need for asymmetric cryptography, the RSA algorithm with a small exponent (unfortunately not secure enough) or algorithms based on Rabin cipher (onerous in software implementation) are the most commonly used [3].

Symmetric cryptography, also called private (secret) key cryptography, includes the group of algorithms which use the same key for encryption and decryption procedure. The key is shared by both communicating sides and has to be kept secret. The symmetric cryptography uses block ciphers

as well as stream ciphers. In the first case, the message block with defined length is encrypted, in the second case, each consecutive bit of message is encrypted. Practically, the block ciphers exploiting substitutions and permutations in the form of Feistel networks are mainly used. The most important feature of such ciphers is the fact, that the same structure (function) can be used for the encryption as well as the decryption. This significantly simplifies and lowers the costs of the algorithm implementation (by software or hardware means) [4, 5]. Due to this fact, 3DES and DESX algorithms, well-known but not too secure, are often used to assure confidentiality in the distributed measurement and control systems. On the other hand, in the distributed system requiring an especially high security level, the hardware circuits implementing AES algorithm are used, which until now was a safe option. The hardware implementation is strongly optimised to achieve high execution speed and energy consumption efficiency, but it is unfortunately rather expensive. Alternatively, the TEA family algorithms [3] could be used, a very interesting, but still not so popular safety solution for the distributed systems.

Tiny Encryption Algorithm (TEA) is symmetric block cipher developed by Cambridge University, and for the first time presented on Leuven workshops considering encryption algorithms with fast software implementation [6]. The TEA algorithm operates on 64-bit data blocks, containing two 32-bit words and the same 128-bit key is used for encryption and decryption. The algorithm has Feistel network structure with 64 rounds, which are organized into 32 pairs called cycles. Consecutive cycles use the same summing, summing modulo 2 and bit-shifting operations, assuring fulfilment of the Shannon property concerning safe block ciphers (diffusion and mixing) [7-8]. The software implementation is very simple and the reference code in C language is given in [6].

The simple algorithm together with a high number of repetitions of non-linear operations should guarantee security and fast execution. Unfortunately, the original TEA algorithm have had a few small defects (the effective key length decreased to 126 bits, increased vulnerability to the attack using related-keys method), which were detected shortly after publication. Due to these disadvantages, the TEA authors had decided to develop new, improved, version of the algorithm called XTEA (Extended TEA), which eliminates detected problems [7-8]. In relation to the original TEA, the changes are cosmetic and concern non-linear operation performed during each round as well as the way of each round subkey generation. Together with the XTEA, the variable block length cipher Block TEA using round function from the XTEA was also published [9]. Because in the newly developed cipher there were shortly found theoretical lacks of security mentioned in [10] and [11], it was decided to develop the third, the newest and, as far, the safest cipher version called XXTEA (Corrected Block TEA).

XXTEA was published in October 1998 and is the block cipher which corrects the security flaws detected in its predecessor. The algorithm uses unbalanced Feistel structure and operates on the data block containing at least two 32-bit words using the 128-bit key for encryption. The data encryption or decryption depends on performing the number of algorithm cycles equal to 6+52/*n*, where *n* determines the number of 32-bit data words in the data block. Each cycle contains *n* rounds. The main difference in relation to the previous versions is based on the fact, that the XXTEA treats the data block as a circular buffer [12]. Each single cycle of the algorithm requires walking through the whole data block and adding to each 32-bit word the result of the given nonlinear round function, which has four arguments: values of the neighbouring words (the preceding and the succeeding), the key and the round number (counter) as shown in Fig. 3.

The very low memory usage, high speed of encryption and relatively high security level (thanks to its specific structure in the form of the unbalanced Feistel network) can be mentioned as the most important features of the XXTEA algorithm. The main strength of the algorithm lays in joining simple arithmetic and bitwise operations with the high number of cycles, making it ideal for implementation and use in the embedded devices designed to work in the distributed measurement and control systems. The XXTEA guarantees low resource usage, low energy consumption, and relatively high communication security. An additional advantage is the fact that the XXTEA is an open algorithm, free of patent restriction and may be freely implemented in any embedded system.

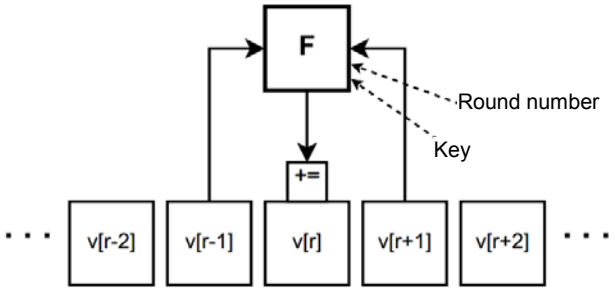

Fig.3. Single operation (round function F) of the XXTEA algorithm

Transmission security assurance in the proposed system

In the discussed system, the data transmission was protected against the unauthorised access with the aid of non-standard use of the XXTEA algorithm. Function **btea()** encrypts and decrypts the measurement and control data. The function has 3 input arguments: the pointer to the table containing the data to encrypt (or decrypt), number *n* defining the input data size (number of 32-bit words) and the function direction (e.g. 3-element table encryption needs to set *n* = 3, but for decryption *n* = -3), a table *key*[4] containing four 32-bit words which define private 128-bit key for encryption and decryption.

Due to minimal input data size limitation to 64 bits (8 bytes) for the XXTEA algorithm, it was proposed to modify the original algorithm. Each 6 bytes of useful information were stuffed with two bytes of random values, thus increasing the encryption security. The random data was obtained by joining the information from pseudo-random number generator - rand() with the variable results of the measurement of the temperature sensor and the supply voltage. Additionally, the pseudo-random number generator is initialised with different seed from RTC clock registers every time the microcontroller wakes up and leaves the low-power STANDBY mode. The random bytes are discarded during data processing in the receiver.

The research presented in [12] shows that the XXTEA algorithm has a strong avalanche effect, e.g. a minimal change in the input data block causes completely different encrypted data contents, which is a welcomed feature of the algorithm from the transmission security point of view. Adding random data to each transmitted information causes, even for two identical messages, the encrypted and the sent data to be practically uncorrelated thus making cryptoanalysis much harder. The random data is not stored at any processing stage, so the cipher key breaking on the basis of the acquisition of defined number of pairs of the

open-text and the encrypted message is practically impossible. The cryptoanalyzer, in fact, has only a part of the open-text, it means, it does not know all the data used for generating encrypted messages, which were captured. The above presented XXTEA algorithm modification causes the best, till now, known attack on the security of the XXTEA, published in 2010 by Elias Yarrkov [12], to be rendered almost useless. The XXTEA algorithm breaking method is based on differential cryptoanalysis and requires collecting ca. 2^{59} pairs of open-text–encrypted message. As the full open-text is not available (even to the system administrator), the key breaking is very difficult, at least until more effective XXTEA attack method will be developed.

Thanks to processing effectiveness of the XXTEA algorithm, the encryption and decryption are very fast. In the realized prototype, based on STM32Fx family microcontroller equipped with Cortex-M core, for selected blocks length, the ciphering times are presented in Table 1. The memory footprint for the function **btea()** is also relatively small and does not exceed 400 bytes. The encryption and decryption are performed "in-place", so there is no need for additional data memory space.

Table 1. The encryption and decryption times obtained in the realized prototype of the presented system

Data block size [B]	Encryption time [ms]	Decryption time [ms]
8	0,512	0,461
16	0,534	0,490
32	0,618	0,573
64	0,866	0,806
128	1,289	1,200
256	2,146	1,998
512	4,210	3,918
1024	8,338	7,758
2048	16,594	15,438

Conclusions

In the first stage, the theoretical background of the distributed measurement and control systems were analysed, special attention was given to the security of the transmitted information inside the system. Next, the proposed system architecture was described, taking into account logical organization of all functional blocks. The known methods for data security were classified and shortly described. In order to achieve required goals, the security procedures were implemented in case of the remote user authentication as well as in the case of ciphering of wireless data transmission between all system components. The main unit of the system and exemplary modules (local and remote) were assembled and tested. The designed device was optimised to achieve minimal power consumption. Final tests have allowed to experimentally prove the effectiveness of the assumed solutions. The presented distributed measurement and control system can be mainly used where there is an application need for easy remote access and wireless transmission security. As an example, the distributed system for mobile monitoring (e.g. steel construction stresses measurement, road traffic intensity estimation) can be given. The implemented cryptographic algorithm allows encrypting the data on each stage of processing, assuring the high security of the data transmission and information storage.

***Authors**: dr hab. inż. Grzegorz Lentka, Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics, Department of Metrology and Optoelectronics, ul. Narutowicza 11/12, 80-233 Gdańsk, E-mail: lentka@eti.pg.gda.pl; mgr inż. Sławomir Tyborczyk, Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics, Department of Metrology and Optoelectronics, ul. Narutowicza 11/12, 80-233 Gdańsk, E-mail: <sla.tyb@gmail.com> .*

REFERENCES

[1] Nawrocki W., Rozproszone systemy pomiarowe, *WKiŁ*, Warszawa 2006.
[2] Winiecki W., Adamski T., Bobiński P., Łukaszewski R., Bezpieczeństwo rozproszonych systemów pomiarowo - sterujących (RSPS), *Przegląd Elektrotechniczny*, 84 (2008), No. 5, 220-227.
[3] Adamski T., Algorytmy kryptograficzne w rozproszonych systemach pomiarowo - sterujących. *Przegląd Elektrotechniczny*, 84 (2008), No. 5, 273-276.
[4] Menezes A., van Oorschot P., Vanstone S., Łukaszewski R., Handbook of Applied Cryptography, CRC Press, Boca Raton 1996.
[5] Schneier B., Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C. Wydawnictwa Naukowo – Techniczne, Warszawa 2002.
[6] Wheeler D., Needham R., TEA, a tiny encryption algorithm, *Fast Software Encryption, Second International Workshop*, 16 December 1994, Leuven, Belgia, 363-366.
[7] Williams D., The Tiny Encryption Algorithm. Columbus State University, Columbus 2008.
[8] Reddy Andem V., A Cryptanalysis of the Tiny Encryption Algorithm. University of Alabama, Tuscaloosa 2003.
[9] Wheeler D., Needham R., TEA extensions. Cambridge University, Cambridge 1997.
[10] Saarinen M.-J., Cryptanalysis of Block TEA. http://mjos.fi/doc/saarinen_block_tea.pdf.
[11] Lu J., Related-key rectangle attack on 36 rounds of the XTEA block cipher. *International Journal of Information Security*, 8 (2009) No 1, 1-11.
[12] Yarrkov E., Cryptanalysis of XXTEA. https://eprint.iacr.org/2010/254.pdf.