Security network interface for alarm systems

Pavlo Bykovyy a, Volodymyr Kochan a, Anatoly Sachenko a, Serkan Aksoy b, George Markowsky c

a Research Institute of Intelligent Computer Systems, Ternopil National Economic University, 3 Peremoga Square, 46009 Ternopil, Ukraine
b Gebze Institute of Technology, Electronics Engineering Department, Gebze, Kocaeli, Turkey
c Department of Computer Science, Orono, ME, USA

A R T I C L E    I N F O
Available online 3 November 2011

Keywords:
- Sensor networks
- Alarm systems
- Serial network interface
- Network security
- Multiplexed networks

A B S T R A C T
Authors suggested the development of a specialized network interface for network of detectors that are part of alarm system. Providing a high level of network security against intruder is achieved using a large number of security elements and their dynamic change in on-line mode network operation. The proposed system uses traditional detectors; each is connected to the network through node based on a microcontroller. This allows connection of traditional detectors into two-wired network with common bus type, and to reduce the number of wired lines without loss of system informative channels. An additional advantage is in powering sensors by a server via informational network channel.

© 2011 Elsevier B.V. All rights reserved.

1. Introduction

Developed by authors CAD for alarm systems optimization [1] allowed to identify the benefits of common bus topology, unlike the traditional star topology of such kind of systems, since in many cases the costs of cabling may be the same as detectors costs. Using network sensors increases the cost of the system [2] and wireless detectors has higher prices and worse noise stability. In this case we have contradictory situation in selecting of the most cost-effective alarm system structure. Analysis showed that more economical will be network topology based on a common bus cheap traditional detectors equipped with appropriate network adapters [3,4]. For its construction it is necessary to select an interface which should provide: (a) information exchange between detectors and network server using cheap two wired line; (b) provide power to traditional sensors using the same informational wires, (c) provide protection from intruder. Analysis of the commonly used serial interfaces showed that they do not meet the proposed requirements. In particular, RS232 and SPI are not for network usage, LIN does not provide power to the sensors, RS485 and CAN require expensive twisted pair cabling. I2C is designed for small distances [5,6]. The best base would be 1-Wire interface, but it provides a power only for special low-power devices. Therefore it is expedient to develop a special interface, similar to 1-Wire.

During the point (c) performance, it should be noted that the required length of detectors messages is pretty small (a few bits only), which is not allowing to implement reliable protection using regular cryptographic methods. In this case it is expedient to increase the length of detectors messages, (but not too much), in our case, the message length in 20 bits is enough.

To provide high network security against intruder it is necessary to complicate the possibility of one or more detectors [or network in general] emulation by him. To perform such simulation an intruder needs to decrypt data exchange procedures. All decrypting methods are based on the analysis of individual messages, so to protect the system one should: (i) to hide the source of detectors signals in the network, (ii) to hide the structure of messages, (iii) often change of the security settings in on-line mode (with a period of several minutes).

Microcontroller interfaces are standard [5-7], that’s why they can’t accomplish provided requirements. Therefore, it is expedient a program implementation of specialized interface that will allow to implement mentioned methods of network security and flexible changes of separate interface parameters as well as certain set of them. To implement this interface one should hold an analysis of serial interface elements that could be used to secure messages in the detectors network of alarm system.

2. Security elements of proposed interface

In general, from intruder side, the serial interface can be represented as a bit stream in the network that follows one by one in time. For cracking it will be necessary: (i) to select the bits of separate devices (assign certain bits to appropriate detectors or network server); (ii) to assemble a separate messages (place every bit into its place); (iii) to learn how to imitate detectors messages of that has no alert signal; (iv) to learn how to imitate the work of detector in the network (correct response to the server requests); (v) to learn how to distinguish the changes between interface parameters; (vi) to learn how to modify the interface parameters according to appropriate requests.

E-mail addresses: saksoy@gyte.edu.tr (S. Aksoy), markov@maine.edu (G. Markowsky).

0920-5489/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
To achieve the provided task of securing detectors’ network it is necessary to create difficulties for intruder in all stages of network breaking. As a basis for security it is appropriate to use pseudo-random number generators that are easy provide in software implementation. Thus, for certain security features it is appropriate to use individual generators, rotation period of which are relatively prime.

Detailed analysis of serial interfaces showed that security elements can be divided into three groups: (i) the impulse parameters transmitted through the network, (ii) the cipher variants during the encrypted messages transmissions, (iii) the order of sending messages. The specific combination of elements is defined by server’s microcontroller (SMC) of the network for each detector.

Security features for the first group of security elements, the impulse parameters transmitted through the network, might include:
1) creating a continuous stream of standardized impulses in the network to complicate the detection of impulse sources,
2) pseudo-randomly changing the data exchange frequency,
3) pseudo-randomly changing the number of bits in the detector’s response,
4) pseudo-randomly changing the number of bits in the server’s request,
5) pseudo-randomly changing the number of informational bits in the detector’s response,
6) pseudo-randomly changing the number of informational bits in the server’s request,
7) pseudo-randomly changing the position of the informational bits in the detector’s response,
8) pseudo-randomly changing the position of the informational bits in the server’s request.

Security features for the second group of security elements, the cipher variants during the encrypted messages transmissions, might include:
1) pseudo-randomly changing the detector’s logical numbers,
2) using crypto algorithms based on pseudo-random number generators to encrypt the detector’s informational messages,
3) using multiple variants of the server’s query,
4) using multiple variants of the detector’s response,
5) pseudo-randomly changing the detector’s encryption algorithm for informational messages,
6) pseudo-randomly changing the number of bits in the real message,
7) frequently (every few minutes) changing the pseudo-random number generator parameters,
8) using pseudo-random number generators that have relatively prime repeat periods.

Security features for the third group of elements, the order of sending messages, might include:
1) periodically changing consequent and group questioning of detectors,
2) pseudo-randomly changing group order during group questioning of detectors,
3) pseudo-randomly including different detectors into the group,
4) cycling the order of the bits from different detectors messages in the group message.

Furthermore, it is reasonable to change the security elements parameters during network performance (or separate detectors) mode “not under guard” of object (e.g., customer services in some certain room of the bank) to the mode “under guard”. When traditional detector is in the “not under guard” mode, it still generates alarms signals through appropriate channels if his sensing elements are triggered, but network server doesn’t respond to it in case of selected mode. It means that it is easily to create situations in the network that are imitation detectors alarm signals in specified channels (while intruder has legitimate access to the protected by detectors areas) and collect data about network work using special registering device (this device is passive and doesn’t send any signals to the network, so it’s installation by intruder should also be taken into account). This situation, from the cryptography point meets the condition in which the attacker knows a part of the message, which significantly facilitates breaking the network.

In this case, changing the parameters of security elements during the changes of alarm systems modes will disorientate intruder. In “not under guard” mode it is expedient to transmit not associated with triggered sensing elements in detector alarms but random signals, thus the state of network security in cryptography terms remains the situation when intruder doesn’t know any of messages (but may think that he knows it). Last feature allows creation a trap for intruder - while the alarm system uses “not under guard” mode it is used pretty simple security elements that intruder may break which will provoke him to active actions and allows to detect his presence.

3. Hardware tools of proposed interface

3.1. Time-schedule of network performance

The requirements of pulse messages standardization don’t allow to use the pulses of network server requests to power detectors

<table>
<thead>
<tr>
<th>Table 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timing of bits in the network.</strong></td>
</tr>
<tr>
<td>Interval</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td>12</td>
</tr>
</tbody>
</table>

Fig. 1. Impulses time diagram in detector’s network.

---

P. Bykovyy et al. / Computer Standards & Interfaces 34 (2012) 468–475

469
because the amplitude of pulse power signals (and detector responses) depends on voltage drop on network resistance. Therefore it is expedient to separate the detector’s power impulses from informational impulses of the message.

Impulses time diagram in detector’s network is presented in Fig. 1. In spite of pulse power impulses stand out from the network bit stream, informational bits of the server and all detectors have the same parameters. Therefore it is difficult for intruder (without special implementation of resistors into different parts of the network and cross-withdrawal of data pulses, which requires a long time physical access to the network wires) to select which of the impulses are server commands or detectors response, as well as what detector is sending a message at current moment.

Impulse amplitude was selected about 11÷12 V according to the voltage of backup power battery of server. In this case, impulse that provide power for detectors is appropriate to choose as dual to backup power, in order to generate them using the accumulate circuit, where capacitor for the time of passing messages through powerful MOS-keys is connected to server’s power, and for the time of impulse power generation for detectors power supply it is connected with other powerful MOS-keys of the network sequentially with supply voltage of server. In this case the maximum number of detectors in one branch of the network is defined by output current, which may be issued by server to provide power for detectors. Cheap MOS-keys allows to connect, for example, up to 20 detectors with regular current supply up to 30 mA per line branch, which completely satisfies most of consumers.

Table 1. Sequence of bits appearance in the network.

Sending of individual message bits into the network by detector, which is part of a group, is defined by one of the tables of answers order that are written into microcontrollers memory that are connected to the detectors of the network. They are created randomly by network server during the network initialization process. They are noncontradictory (at one time may response only one detector) and are periodically changing in the group according to order provided in server’s request.

3.2. Network and detector structure

Fig. 2 shows the general structure of proposed alarm system, which consists of n detectors (up to 10...20 per one branch) connected to the local two-wired bus using microcontroller units MC1...MCn[3,4] that are placed inside detectors cover. Bus is also connected to Servers MC unit that is querying detectors using connected to them MC1...MCn. Servers MC is also providing functioning of detectors by regular sending to the network power impulses. In case of alarm, the signal is transmitted from detector to its microcontroller and then to the server that provides appropriate reaction into this alarm using informational devices connected by other local bus to server. Software implementation of the proposed interface cause additional resources however it allows to provide all proposed element of security.

The structural scheme of microcontroller unit that is connected to regular detectors of alarm systems and transmit their state is presented on Fig. 3. It consists of stabilizers ST1 (12 V) and ST2 (5 V), interface receive unit and transmit unit, regular detector connected to microcontroller.

Power supply impulses that are going through the diode are charging capacitor, its output voltage is provided to power detectors and transmitter stabilizer (ST1) and microcontroller stabilizer (ST2). Its entrance is fixed by built into microcontroller comparator and its interruptions are synchronizing microcontroller’s work, so embedded into microcontroller RC-generator may be used instead of quartz which will reduce the price of whole unit.

In the scheme on Fig. 3 traditional detector is powered by normal for him stabilized voltage +12 V, which also determines impulses
Fig. 4. Circuit diagram of microcontroller unit that connects to the detector.

Fig. 5. Circuit diagram of the network server.
amplitude that are sent to the network. Therefore their small amplitude is determined by small scattering of output voltages ST1, and not by detector’s place in the network (as it was in [3,4]), which implements the first element of security.

Voltage from the output ST2 comes also to the receiver unit, which limits the amplitude of incoming impulses from the network to an acceptable for microcontroller +5 V level. Furthermore, this voltage is used to form the comparator’s reference voltage, which selects power impulses of detectors.

On Fig. 4, is presented a circuit of microcontroller unit that includes a microcontroller U1 of type ATmega16, reset circuit (R3, C5), the power supply (D2, U3, U4, C1, C2, C3), receiver (R1, R2, C4, Q1), transmitter (R8-R10, Q2, Q3), reference voltage divider (R4, R5) and impulse voltage divider (R6, R7), detector connections to microcontroller (PB4-PB7).

A circuit diagram of the network server is presented on Fig. 5. It is based on the ATmega128 microcontroller (U2) and also includes reset circuit (C8, R21), quartz resonator (X1), receiver (R28-R30, Q9, C10), transmitter (R25-R27, Q6, Q8, D5), power supply impulses generator (R22-R24, Q4, Q5, D4). The server is providing 24 V power supply impulses for powering detectors and microcontroller units and their synchronization. The informational signals – servers commands and detectors answers have 12 V.

4. Working algorithms of connected to detectors microcontrollers units

The program of microcontroller work, consists of three modules — the main one, comparator interrupts requests processing module and timer interrupt processing module.

After the initial setup of microcontroller unit the main module implements only wait for comparator’s interrupt cycle.

In Fig. 6 is presented the algorithm of comparator interrupts requests processing. During its performance is made a timer T0 synchronization which sets the time chart of microcontroller’s work and recognition of server requests, its type, and if it is necessary — the parameters of group mode querying. In addition, the survey of detectors inputs PB4 – PB7 (see Fig. 4). Parameters of pseudorandom number generators are changed simultaneously, according to the generated tables that are saved into the microcontroller’s memory during initialization procedure.

In the Fig. 7 is presented the algorithm for timer T0 interrupts requests processing, which sets the time chart of the microcontroller work. This timer T0 is reconfiguring from power impulses width to message impulses duration. According to the mode of server’s bits requests receiving or the bits formation of own message, it is conducted frequent querying of receiver outputs (Q1, see Fig. 4) or providing to the transmitter inputs (D2, see Fig. 4) of corresponding logical levels. At the end of receiving server’s request it is recognized beginning of a new cycle of sensors querying (the server passes all 1…1) or server query that contains information about the querying of the specific detector or parameters of group query. In the last case, microcontroller according to provided to him code table, defines the number of bits that he should form in a group and resets bits counter in the group.

5. Pseudo-random number generators

In case of limited budget microcontrollers usage the used pseudorandom number generators should have a simple implementation and provide easy change of parameters in on-line mode. These requirements fulfill a combination of linear recurrent registers, where each represents a shift feedback register combined by module 2 [9,10]. It’s software implementation is easy, they can provide a wide range of pseudo-random numbers with a large period of code combinations repeating.

6. Network initialization procedure

The main purpose of the initialization procedure is work coordination of all microcontrollers that are included into the network. During its performance for each MC1 … MCn is provided: (i) their individual numbers in the network (in order not to use long factory serial number, which would reduce the network security), (ii) individual initial parameters of pseudo-random number generators, (iii) a set of individual
code tables, according to which each $MC_1 \ldots MC_n$ should determine numbers of bits that during group performance process should be created by him. Also during initialization process the modules memory protection bits $MK_1 \ldots MK_n$ are saved.

As can be seen, during initialization procedure to $MC_1 \ldots MC_n$ are send secret data. Therefore, access to initialization procedure must be strictly limited. For this proposed network uses the following points: (i) all algorithms of $MC_1 \ldots MC_n$ detector’s individual number formation, parameters of pseudo-random number generators and code tables are contained in the Server’s MC and can’t be read by any other person, (ii) before the initialization procedure the network administrator authentication process is made, (iii) current set of security elements that will be used for providing network security choose network administrator based on the general list (see Section 2), (iv) the detector’s initialization is made by a separate port of server which has protection from physical access and network administrator seal; (v) initialization procedure is performed for all detectors in the network consistently, without breaks, (vi) network expansion or modernization requires the network initialization procedure again.

The last requirement ensures maximum protection against possible replacement of the detector during initialization process by intruder. However, it is not preferable when the network configuration changes frequently. Therefore, we can provide a portable initialization block that during network expansion or modernization provides initialization

---

**Fig. 7.** The algorithm for timer T0 interrupts requests processing.
of all sensors on their current place, as well as a network server. This unit is saved by the administrator with access is restricted password.

7. Practical implementation

The proposed technical solutions were tested on a test board network. Fig. 8 presents the layout of the proposed alarm system.

In the proposed layout test board of alarm system the outputs of each detector (5) are connected to the appropriate network controller (6) through two-wired network (7) which is connected to a network server (2). Power supply unit (1) forms the server data acquisition board and detectors of the network. To control and setup modes of alarm system work is used membrane keyboard (3). To display information about the state of detectors is used display on liquid crystals (4).

Detectors microcontroller unit (see Fig. 8) is implemented as a test board (6) based microcontroller ATmega16. Network server unit (2) is implemented on the basis of ATmega128 microcontroller. In a two-wired network one line is used to transmit informational signals and power signals (see Fig. 3) and another line - ground.

9. Conclusions

We propose a specialized interface for detectors network of alarm system that allows providing high level of network security inside alarm system using a large number of security elements and their dynamic change in on-line mode as well as a low cost design that significantly reduces the amount of cabling necessary.

Acknowledgments

The authors would like to thank the Ministry of Education and Science of Ukraine and the Scientific and Technical Research Council of Turkey (TUBITAK) for supporting this paper as part of the joint Ukrainian-Turkey project M/47-2008 entitled “Design and Optimization Methods of Physical Intrusion Detection for Security Systems”.

References


Bykovyy, Pavlo is a lecturer, PhD at the Information Computing Systems and Control Department of the Ternopil National Economic University. He received a B.Eng. degree in Computer Engineering at Ternopil Academy of National Economy in 2004, specialist degree in Computer Systems and Networks at Ternopil State Economic University in 2005, and PhD degree in Computer Systems and Components at Ternopil National Economic University in 2011. His research interests include Computer Systems and Networks, Software Engineering, Sensor Networks, and Alarm Systems.

Kochan, Volodymyr is an Associate Professor of Information Computing Systems and Control Department, Director of Research Institute of Intelligent Computer Systems at Ternopil National Economic University. He received a B.Eng. degree in Electrical Engineering at Lviv Polytechnic Institute in 1973 and PhD degree in Electric and Magnetic Instrumentation at Kiev Polytechnic Institute in 1989. His research areas include Sensor Intelligent System; Distributed Sensor Network; Computer Based Intelligent Measurement and Control Systems; Intelligent Controllers for Automated and Robotic Systems in Industry; Sensor Systems Calibration and Verification.
Sachenko, Anatoly is a Professor and Head of the Department of Information Computing Systems and Control, Director of American-Ukrainian Program in Computer Science at Ternopil National Economic University. He received B.Eng. degree in Electrical Engineering at Lviv Polytechnic Institute in 1968, and PhD degree in Electrical Engineering at Lviv Physics and Mechanics Institute in 1978, and Doctor of Technical Sciences degree in Electrical and Computer Engineering at Leningrad Electrotechnic Institute in 1988. Since 1991 he has been an Honored Inventor of Ukraine, and since 1993 he has been IEEE Senior Member. His main areas of research interest are Implementation of Artificial Neural Network, Intelligent Distributed System and Network, Parallel Computing, and Intelligent Controllers for Automated and Robotics Systems.

Aksoy, Serkan is an Associate Professor, Doctor of Electronics Engineering Department at Gebze Institute of Technology and a Part-Time Researcher involved in various projects of The Scientific and Technical Research Council of Turkey (TUBITAK). He received a B.S. degree in Electronics and Communication Engineering from Istanbul Technical University, Turkey, in 1996, and M.S. and PhD degrees in Electronics Engineering at Gebze Institute of Technology, Turkey, in 1999 and 2003, respectively. His scientific interest includes Analytical and Numerical Time-domain Solutions of Electromagnetic and Underwater Acoustic Wave Propagation Problems.

Markowsky, George is a Professor of Computer Science, a Chair of the Computer Science Department and a President of Ayers Island, LLC. He received a BA in Mathematics from Columbia University in 1968, M.S. in 1969 and PhD in 1973 in Mathematics at Harvard University. His interests range from pure mathematics to the application of mathematics and computer science to biological problems.