Data Communication Crypto Protocol for Security Systems
Sensor Networks

P. Bykovyy¹, V. Kochan¹, Y. Kinakh¹, A. Sachenko¹, O. Roshchupkin³, S. Aksoy³, G. Markowsky⁴
¹ Ternopil National Economic University, Research Institute of Intelligent Computer Systems
Ternopil, Ukraine, E-mail: pb@tneu.edu.ua
² Chernivtsi National University, Computer Science Faculty
Chernivtsi, Ukraine, E-mail: alrosh@rambler.ru
³ Gebze Institute of Technology, Electronics Engineering Department
Gebze, Kocaeli, Turkey, E-mail: saksoy@gyte.edu.tr
⁴ Department of Computer Science
Orono, ME, USA, E-mail: markov@maine.edu

Abstract – This paper describes hardware implementations of crypto protocol elements for secured data communication in two wired networks of security system detectors. Those elements are basic to crypto protocol development for that type of network. In addition, hardware tools for the network controller and the network server that support this protocol were developed. These tools will allow us to test and debug the proposed security elements and the crypto protocol.

Keywords - security systems, sensor networks, crypto protocol, microcontroller

I. INTRODUCTION

Traditional security systems detectors have some mix of normally closed (NC) and normally opened (NO) contacts each with 2 kΩ nominal resistance. They expect that each sensing element (sensor) in the system will be connected to its own separate socket (zone) in the alarm control panel (star topology). For complicated networks, this requires a large number of cables [1, 2]. By basing a system on computer network technology we can substantially reduce the number of cables [3, 4], but, in general, such systems are expensive [5]. According to [1, 2], the least expensive way to integrate network technology into such a system is by incorporating microcontrollers into the detectors themselves. Such a microcontroller converts a detector’s signals into a coded message and also serves as a power supply by receiving power through the communications network. By using a crypto protocol between the microcontroller in the sensor and the main network it is possible to thwart many types of attacks including the attacks that spoof the signals produced by the detectors. Most standard crypto security systems fail when the lengths of the server informational messages are small (1...3 bytes). Therefore, it is reasonable to develop a special crypto protocol that can be used in networks that are based on the controllers proposed in [1, 2]. Before we develop the protocol, we will consider the structure of the proposed security sensor network.

II. GENERAL STRUCTURE OF SECURITY SENSOR NETWORK

Figure 1 shows the structure of our proposed security sensor network, which consists of n detectors connected to the local two-wired bus using microcontrollers MC1…MCn.

![Diagram of the proposed security sensor network](image-url)

This structure allows us to reduce the number of communication lines by changing the standard security system star topology into a bus topology. Moreover to prevent intruders from being able to simulate detectors being disconnected, we need to provide cryptographic security to the communication protocol. In general, a
security system would have a variety of sensors and communication elements. Because the standard RS-232 interface [1, 2] is relatively simple, we can create a lightweight security protocol. To handle the protocol efficiently we must also create a software interface [6 - 8]. For security concerns data part of such a protocol packet should have at least 30 bits. Implementing the software interface requires additional effort, but it increases the security of the protocol. The server's microcontroller (SMC) provides the cryptographic functions necessary for the security of the network. The microcontroller powers the sensors by sending continuous signals that charge capacitors located in the detectors.

The output of built-in in SMC RS232 interface is used to connect the server to the indicator panel, personal computer, LED with keypad and other elements such as the alarm (siren) controller.

### III. THE ELEMENTS OF THE CRYPTO PROTOCOL

Analysis of the features of some common and inexpensive microcontrollers showed that a software implementation of the interface would allow us to maximize the usage of different elements of the crypto protocol. It would also provide flexibility in configuring the various protocol elements. The following set of security elements could be used in our protocol to prevent an intruder from imitating the disconnection of detectors:

1. impulse parameters transmitted through the network,
2. transmitting encrypted variants of messages,
3. modifying the order of messages.

A unique combination of security elements should be set by the SMC for each microcontroller whenever possible. Security features for the first group of security elements, the impulse parameters, 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 microcontroller'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 microcontroller'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 microcontroller'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, might include:

1. pseudo-randomly changing the microcontrollers' logical numbers,
2. using crypto algorithms based on pseudo-random number generators to encrypt the microcontroller informational messages,
3. using multiple variants of the server's query,
4. using multiple variants of the microcontroller's response,
5. pseudo-randomly changing the microcontroller'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 microcontrollers,
2. pseudo-randomly changing group order during group questioning of microcontrollers,
3. pseudo-randomly including different microcontrollers the group,
4. cycling the order of the bits from different microcontroller messages in the group message.

Such a huge number of features in the three groups of security elements provides reliable security for the network under a wide variety of conditions.

Our protocol uses a notebook cipher algorithm to increase the crypto security of network protocol communication in the local server-microcontroller bus.

The security of our protocol depends on a pseudo-random number generator that generates the cryptographic key. It is known that the generator should provide high structural secrecy by producing uniform pseudo-random numbers that don’t depend on the previous elements of the pseudo-random sequence. To determine the cryptographic stability of the proposed structure it is necessary to use a mathematical model [9]

\[
I_{6} = \frac{N_{var} P_{r}}{\gamma}
\]

where \(N_{var}\) is the number of variants necessary to implement cryptanalysis, \(\gamma\) is the system productivity, \(P_{r}\) is the probability of successful cryptanalysis, and \(I_{6}\) is the expected system breaking time if \(P_{r} = 1\).

The appropriate equations in cylindrical coordinates can written as :

\[
\begin{align*}
N_{var} &= \rho \cos \varphi \\
\gamma &= \rho \sin \varphi \\
z &= I_{6}
\end{align*}
\]
where $\rho = \sqrt{N_{\text{var}}^2 + \gamma^2}$, and $\varphi = \arctan\left(\frac{N_{\text{var}}}{\gamma}\right)$.

The results of experiments with key length are shown in Figure 2. Research shows that increasing of the key length will considerably increase the time required for cryptoanalysis. In particular, a key of 256 bits being analyzed at 1 GHz will require the following amount of time for success:

$$t = \frac{2^{256} - 1}{10^{12} \times 3 \times 10^7} = \frac{10^{76.8}}{3 \times 10^{19}} = 3.3 \times 10^{56.8} \approx 10^{57} \text{ years}$$

Fig. 2. Cryptographic resistance of the generator.

Linear recurrent registers (LRRs) for unique pseudo-random sequences are often used in practice. LRRs are small, simple and inexpensive devices that can provide a large number of sequences and satisfy the following requirements:

- they can generate a huge number of sequence families based on the same algorithm,
- they optimize the cross-correlation functions in the family,
- they provide structural balance,
- they maximize the period for the size of the shift register.

The FIPS 140-1 standard specifies four statistical tests of randomness: the monolith test, the block test, the series test, and the test of series lengths. The ranges of statistical parameters are set for these tests. A sequence of 20,000 bits produced by the generator being tested is enough for each of four tests in the standard. A generator must pass all four tests to be certified under this standard.

IV. CRYPTO PROTOCOL IMPLEMENTATION

In order to provide a high level of cryptographic security it is necessary to make it difficult for an intruder to spoof one or more microcontrollers with detectors being disconnected. Such spoofing requires the intruder to decrypt the data communication protocol. All decryption methods are based on the analysis of separate messages, so that hiding the source of signals complicates the analysis. This feature was not implemented in [1, 2]. In our current implementation, we separate the microcontroller’s power impulses and the informational message impulses. The timing-chart of the impulses is shown in Figure 3.

Fig. 3. Time-chart of impulses in the sensor network.

The hardware implementation of our crypto protocol is shown in Figure 4. It consists of detectors connected to microcontrollers that transmit the state of the detectors. Whenever the server requests a detector’s state, the microcontroller retrieves the state of the sensing elements of the detector and sends the response through the transmitter.

Fig. 4. Hardware structure of the our crypto protocol.
The main feature presented in Figure 4 is the power supply system. It consists of a diode and a capacitor that form a constant voltage power supply by periodically recharging the capacitor using server impulses. The detector is powered by Stabilizer 1 (ST 1) with its voltage of +12 volts. The same voltage is applied to the message transmitter and defines the amplitude of its output impulses. The diode does not conduct during the message transmission in case the capacitor in the power supply circuit is charged to a higher voltage than the transmitter output. Thus, network loading falls sharply during message transmission. The voltage drop on the line between the detector and server becomes less than the stabilization voltage spread by Stabilizers 1. This permits analysis that can identify the message source by the amplitude of the impulses analysis.

The microcontroller is powered by +5V voltage of Stabilizer 2 (ST 2). The same voltage is applied to the receiver which limits the network impulse amplitude to the standard microcontroller level of +5V. Also, the +5V voltage serves as the reference voltage for a comparator that extracts the power supply impulses. In addition, the impulse voltage drop of the detectors serves to synchronize the message transmission impulses.

Figure 5 shows the experimental prototype of our security system where each detector (5) is connected to the appropriate network controller (6). Each controller is connected to the alarm panel (2) using a two-wired cable (7). The power supply (1) provides a voltage of +9V to supply the alarm panel, network controllers and detectors. A membrane keypad (3) is used for the management and configuration of the security system. A liquid crystal display (4) is used to display the state of the security system. The network controller is implemented on a debug kit board (6) based on the ATmega16 microcontroller. The alarm panel (2) is implemented on a ATmega128 kit board based on the ATmega128 microcontroller and supports RS-232 and modified RS-232 interfaces that supports the bus topology of Figure 1. A two wire network (one wire carries the information and power signals (see Figure 3) and the other wire is the ground) is implemented on the basis of a modified two-wire interface for RS-232.

We plan to implement the network controller (6) (Figure 5) based on the smaller ATmega88 microcontroller, which will reduce the size of the network controller board and will allow it to fit inside standard detectors.

![Experimental prototype of security system.](image)

V. 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-Turkish project M/47-2008 entitled “Design and Optimization Methods of Physical Intrusion Detection for Security Systems”.

VI. CONCLUSIONS

We propose an architecture for a security sensor network that allows large sensor groups (12...20 units) in a branch of the network. This architecture provides for power to each sensor. This architecture provides a low cost design that significantly reduces the amount of cabling necessary, and also provides a high level of
security against intruders using the crypto protocol that we describe in this paper.

REFERENCES


