Measurement 46 (2013) 4353–4361

Contents lists available at SciVerse ScienceDirect

Measurement

journal homepage: www.elsevier.com/locate/measurement

Analysis of the position-based quantum cryptography usage in the distributed measurement system

Piotr Bilski [a,b,*], Wiesław Winiecki [a]

[a] Institute of Radioelectronics, Warsaw University of Technology, Warsaw, Poland
[b] Faculty of Applied Informatics and Mathematics, Warsaw University of Life Sciences, Warsaw, Poland

ARTICLE INFO

Article history:
Available online 10 June 2013

Keywords:
Quantum cryptography
Distributed measurement systems
Authentication schemes

ABSTRACT

The paper presents the analysis of a secure transmission channel between nodes in the distributed measurement system. Its security is discussed, using the position-based scheme, where each node is authenticated based on its geographical position. To decrease the threat of the adversary disguising as the authorized node and eavesdropping the transmission, the quantum cryptography scheme is used. The paper presents the modifications and practical implementation issues of such a communication scheme in the distributed measurement system. Time measurement accuracy and clock synchronization are considered, as well as technical difficulties in delivering the secure quantum channel in the open space.

1. Introduction

Distributed measurement systems (DMS) became the standard in the automation and control applications. Introduction of the fast computer equipment facilitated creating more universal and flexible approaches. The same microcontrollers or programmable logical controllers (PLC) can be used for multiple purposes, depending on their selected configuration of the software controlling the measurement task. Abilities of the specialized computers allow for increasing the number of measurements taken at each location and processing them on-site. Also, with the rising accessibility to communication media, even the simplest devices contain network interfaces. This increases the range and expands applications of DMS, but also introduces security threats, which may compromise the measurement and control operation [1].

The secure transmission of measurement data is an important topic in the age of terrorism and ubiquitous access to the computer networks. Multiple structures delivering services to the society (power plants, water supply stations, traffic control centers) are now partially or fully automated, which is possible thanks to the reliable and efficient hardware. The rising amount of micro- electromechanical systems (MEMS) will be used to gather multiple measurements and send them to servers through the central cloud-based storage. Unfortunately, this facilitates intruder attacks, aiming at taking control over the system or damaging it beyond repair. Therefore sophisticated cryptographic protocols must be used to prevent compromising the system by the potentially the attacker.

The paper presents the application of the position-based cryptography to ensure safety and integrity of measurement data, transmitted within the DMS. This new idea was already considered for application in distributed systems, including sensory networks [2,3]. To increase security of the system, the quantum cryptography protocol was added to the scheme [4]. The following paper considers applying this methodology to the specific applications of DMS, including measurement and processing nodes. Apart from theoretical aspects, practical problems are also considered here. The architecture and simplified model of the contemporary DMS is in Section 2. Fundamentals of the cryptography for the needs of the DMS are in Section 3. The position-based quantum cryptography key exchange

* Corresponding author at: Institute of Radioelectronics, Warsaw University of Technology, Warsaw, Poland. Tel.: +48 22 234 74 79.
E-mail addresses: pbilski@ire.pw.edu.pl, piotr_bilski@sggw.pl (P. Bilski), W.Winiecki@ire.pw.edu.pl (W. Winiecki).

0263-2241/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.measurement.2013.05.030

protocol is in Section 4, while Section 5 contains practical issues related to the possible implementation of the protocol. Section 6 contains conclusions and future prospects of the proposed scheme.

2. Security of DMS

The contemporary DMS is a versatile heterogenic system, containing various nodes, depending on their purpose and hardware capabilities [5]. There are two categories of nodes: measurement and processing (Fig. 1). The former are responsible for obtaining measurement data from the outside world (represented by System Under Test) and, optionally, processing them immediately. They are sensory networks or specialized compact computers (such as NI CompactRIO), equipped with multiple data acquisition (DAQ) ports. The second group consists of devices responsible for storing and processing data obtained from remote measurement nodes [6]. Such tasks are usually performed by general purpose computers. They can also work as the control nodes, sending commands to the measurement nodes. All mentioned devices are equipped with communication interfaces. To ensure the safety from the outside-world intruders, such a system is usually separated from any widely accessible medium (such as the Internet). As the result, internal security threats remain. Firstly, the intruder can physically take control over the selected node. The operation requires entering the infrastructure, often making hardware modifications. Therefore the simpler method is the interception of the data exchange. It requires only connecting to the transmission medium and acquiring packets sent between nodes.

In industrial applications, critical for the society, specialized and predictable networks are used [7], next to the Ethernet standard computer network. The communication inside is performed using wired or wireless networks. The former are used traditionally and have proven efficient, especially considering the Real-Time conditions and resilience to the additive noise. The wireless technologies are relatively new (such as ZigBee), but are already well established. In all scenarios, it is possible to get inside the infrastructure and intercept the transmission. To avoid this, cryptographic protocols are often a part of the communication standard (IEEE 802.15.4 for ZigBee). In other cases, additional software (such as PGP for Ethernet) or hardware (Scalance from Siemens) must be used.

The computational power of the measurement nodes is limited and additional effort imposed by the cryptographic algorithms may be unacceptably high. This is the case for small microcontrollers or intelligent sensors, powered by batteries. The solution may be the additional module responsible only for encryption of the measured data, which would be safely transmitted to the processing node immediately after acquisition. The problem is the limitation of the power consumed by the remote node. Therefore cryptographic methods must be simple [8]. This problem usually does not exist in the processing node, which is the personal or industrial computer with relatively high computational resources. Contemporary trends of stressing ecological aspects in technology (such as energy scavenging) prefer power-saving methods and algorithms. Therefore efficient cryptographic methods on both sides of communication are preferred.

To discuss the security of the modern DMS we make the following assumptions:

- The attack comes from within the system, which must be physically penetrated.
- The intruder is unable to take control over the nodes directly, but only by sending remote commands.
- The weakest point in the DMS infrastructure is the transmission medium.
- The size of the DMS is limited, ranging from hundreds of meters to a few (3–5) kilometers.

The attacker must use the communication network utilized by the DMS. It is possible by positioning him within the range of the wireless network or by connecting to the

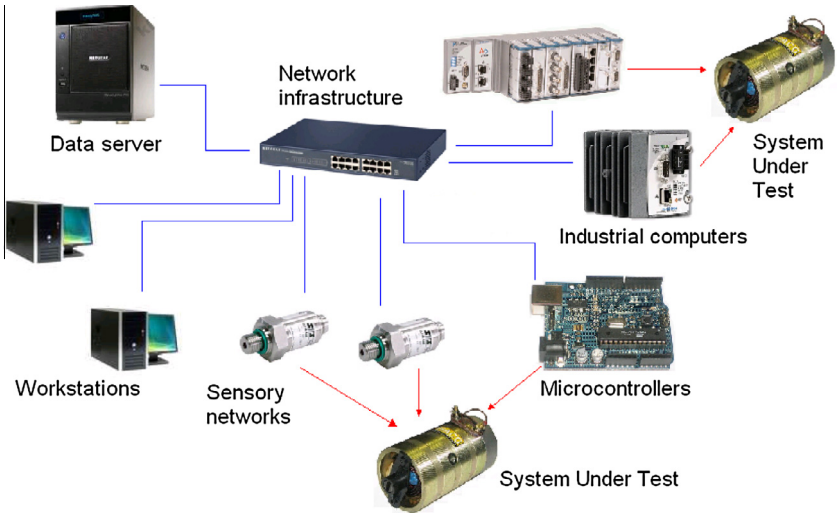

Fig. 1. Architecture of the DMS.