Ad Hoc Networks 11 (2013) 1091–1104

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

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

Security of industrial sensor network-based remote substations in the context of the Internet of Things

Cristina Alcaraz [a], Rodrigo Roman [b], Pablo Najera [a], Javier Lopez [a,*]

[a] Computer Science Department, University of Malaga, Spain
[b] Cryptography and Security Department, Institute for Infocomm Research (I^2R), Singapore

ARTICLE INFO

Article history:
Received 17 July 2012
Received in revised form 30 October 2012
Accepted 1 December 2012
Available online 12 December 2012

Keywords:
The Internet
Supervisory Control and Data Acquisition (SCADA) Systems
Industrial Control Networks
Wireless Sensor Networks
Internet of Things

ABSTRACT

The main objective of remote substations is to provide the central system with sensitive information from critical infrastructures, such as generation, distribution or transmission power systems. Wireless sensor networks have been recently applied in this particular context due to their attractive services and inherent benefits, such as simplicity, reliability and cost savings. However, as the number of control and data acquisition systems that use the Internet infrastructure to connect to substations increases, it is necessary to consider what connectivity model the sensor infrastructure should follow: either completely isolated from the Internet or integrated with it as part of the Internet of Things paradigm. This paper therefore addresses this question by providing a thorough analysis of both security requirements and infrastructural requirements corresponding to all those TCP/IP integration strategies that can be applicable to networks with constrained computational resources.

1. Introduction

The introduction of new technologies and different types of communication systems (Information and Communication Technologies, ICT) in industrial control networks have given rise to new and important advances in the automation and control processes. A particular case is the Supervisory Control and Data Acquisition (SCADA) system, which uses new technologies to monitor in real-time many of the Critical Infrastructures (CIs) deployed in our society, such as energy systems, transport systems or oil/water distribution systems. In particular, Internet connectivity is in high demand as it offers global connectivity and communication, irrespective of the physical location of devices; either industrial engineering devices or communication components.

Fig. 1 depicts a current SCADA system [1,2], where authenticated human operators are authorized to read and manage data streams transmitted by substations. A remote substation is composed of automated electronic devices, known as Remote Terminal Units (RTUs), which are able to collect, manage and resend sensitive data (e.g. temperature, pressure or voltage) received from their sensors to the central system. On the other hand, Fig. 1 also shows how the substations have evolved quickly, trying to adapt new technologies; standing out from among them, Wireless Sensor Networks (WSNs), which are based on industrial sensor nodes and are able to offer control services as an RTU but with a low installation and maintenance cost. Said sensor nodes can be configured in remote substations to supervise, at first level, the natural state of deployed CIs, such as industrial pipelines with water, oil or fuel, as well as electricity pylons or generators. However, current communication standards for this type of technology only contemplate local connectivity, significantly reducing its functionalities out in the field. For this reason, both industry and scientific communities are trying to offer remote

* Corresponding author.
E-mail addresses: alcaraz@lcc.uma.es (C. Alcaraz), rroman@i2r.a-star.edu.sg (R. Roman), najera@lcc.uma.es (P. Najera), jlm@lcc.uma.es (J. Lopez).

1570-8705/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2012.12.001

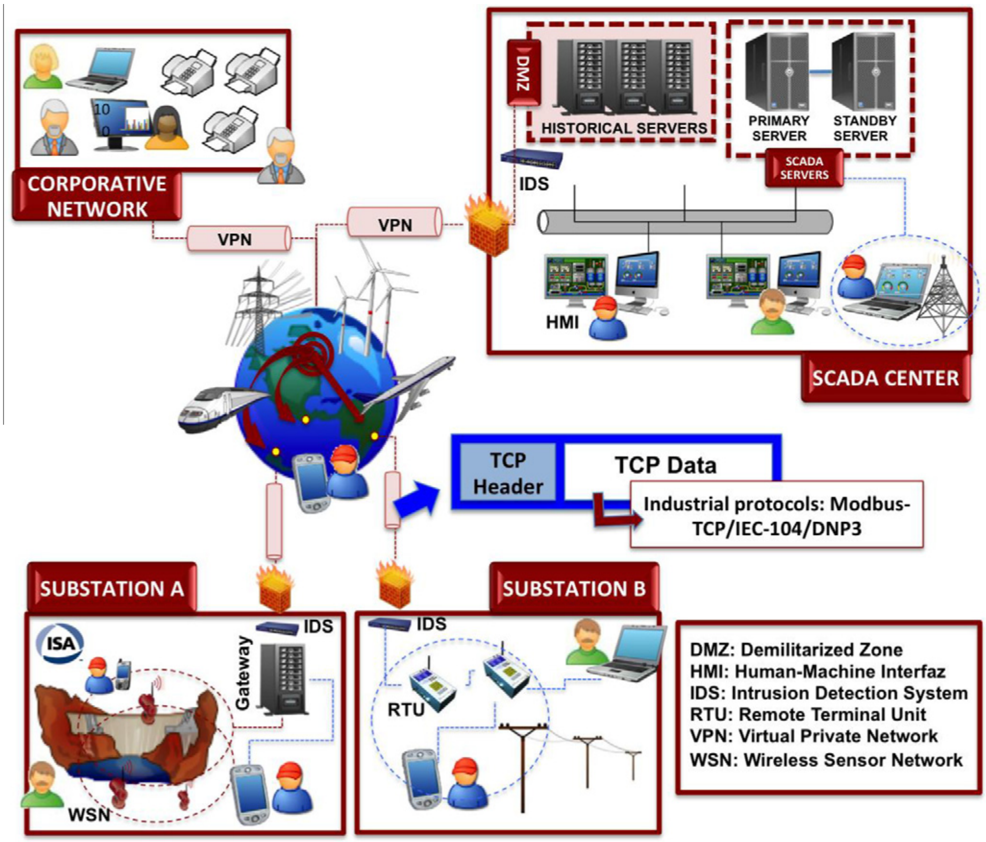

Fig. 1. A current SCADA network architecture.

control and data acquisition through different types of ICTs. As a result, a new paradigm starts to emerge in the context of CI, the Internet of Things (IoT).

The IoT consists of large heterogeneous and interconnected ICT infrastructures, where the Internet, services and physical objects ('Things') play an important role in the control and automation processes. For example, in an industrial context, these things could be industrial sensor nodes, actuators, smart meters, pole-top devices, Radio-Frequency Identification (RFID) tags, Personal Digital Assistants (PDAs), and any other automation devices, such as RTUs [3]. Focusing on WSNs, their sensor nodes will create an autonomous and intelligent virtual layer over the physical environment of remote substations, providing information about the state of the real world that can be accessed from anywhere at any-time. This interaction can be achieved by using many different types of integration strategies: From sensor nodes implementing the TCP/IP stack and becoming fully-fledged citizens of the Internet to capillary networks that maintain their independence, while using Internet servers as interfaces to external entities.

However, it is necessary to study whether the security requirements of critical systems can be fulfilled in this upcoming networks or not. In fact, there are no studies in the literature that provide a systematic analysis of which strategies should be used in the integration of industrial WSNs in the IoT. The purpose of this paper is to provide a basis to try and respond to all these questions; analyzing the security and infrastructural requirements of industrial WSNs connected to the Internet, and discussing the suitability of the integration strategies that will realize the vision of ubiquitous management in the area of control and industrial networks.

The paper is organized as follows. In Section 2, we introduce the advances in remote substation technologies in terms of hardware devices and TCP/IP connectivity. Section 3 explains how the Internet and Wireless connectivity is changing the landscape of industrial control networks. Section 4 describes both the integration strategies and the requirements that have to be considered for achieving a secure integration. Finally, Section 5 provides an analysis of the integration between WSNs and the Internet in the context of control networks taking into account the previously mentioned requirements. Section 6 concludes the paper and outlines future work.

2. Advances in remote substations and communication protocols

The hardware and software (HW/SW) capabilities of RTUs in remote substations have significantly evolved in recent times [4]. In 1970, RTUs used 8-bit microprocessors