A Study of the Evolution of Wireless Communications for SCADA Systems

Minkyu Choi

Security Engineering Research Support Center,
Daejon, Republic of Korea
freeant7@naver.com

Abstract. The Supervisory Control and Data Acquisition systems are collecting data from various sensors nodes deployed in remote locations and then transmitted to a central controller which then manages and controls this data. Utilization of wired or line communications is becoming impractical as the scope is increasing widening. This paper discusses the role of wireless communications for SCADA systems.

Keywords: SCADA systems, wireless communications,

1 Introduction

SCADA (supervisory control and data acquisition) systems are computer controlled systems that monitor and control industrial processes that exist in the physical world [1]. SCADA systems are comprised of computers, controllers, instruments; actuators, networks, and interfaces that manage the control of automated industrial processes and allow analysis of those systems through data collection. These processes include industrial, infrastructure, and facility-based processes, and are used in all types of industries, from electrical distribution systems, to food processing, to facility security alarms [2].

Traditionally, SCADA communication took place over radio, modem, or dedicated serial lines. Today, it is much more common for SCADA communications to travel over LAN or WLAN. Wireless communications can be applied to any setup where a central controller needs to communicate with a remote device or mobile piece of equipment.

In the next sections of this paper, SCADA systems communication is discussed. The conventional installation of the system and the architecture for wireless SCADA are presented.

2 Communications for SCADA Systems

Early Supervisory Control and Data Acquisition (SCADA) system's data acquisition uses strip chart recorders, panels of meters, and lights. Unlike the modern

SCADA systems, there is an operator which manually operates various control knobs exercised supervisory control. These devices are still used to do supervisory control and data acquisition on power generating facilities, plants and factories [4, 5]. Telemetry is automatic transmission and measurement of data from remote sources by wire or radio or other means. It is also used to send commands, programs and receives monitoring information from these remote locations.

SCADA is the combination of telemetry and data acquisition. Supervisory Control and Data Acquisition system is composed of collecting of the information, transferring it to the central site, carrying out any necessary analysis and control and then displaying that information on the operator screens. The required control actions are then passed back to the process [6].

SCADA protocols are designed to be very compact. Many are designed to send information only when the master station polls the RTU. Typical legacy SCADA protocols include Modbus RTU, RP-570, Profibus and Conitel [1]. These communication protocols are all SCADA-vendor specific but are widely adopted and used. Standard protocols are IEC 60870-5-101 or 104, IEC 61850 and DNP3. These communication protocols are standardized and recognized by all major SCADA vendors. Many of these protocols now contain extensions to operate over TCP/IP. Although the use of conventional networking specifications, such as TCP/IP, blurs the line between traditional and industrial networking, they each fulfill fundamentally differing requirements [1].

The process of communication over a SCADA system involves several different SCADA system components. These include the sensors and control relays, Remote Terminal Units (RTUs), SCADA master units, and the overall communication network. Each of these parts is necessary for effective SCADA communication. A system can effectively monitor alarms and status updates within the network only when all of these system components function properly. For more complete monitoring of SCADA communications, operators must deploy advanced RTUs.

The RTU is where most SCADA communication is gathered within the system. Values from inputs and outputs, referred to as SCADA points, and are sent from individual sensors to the RTU. The RTU is responsible for forwarding these SCADA communications to the master station, or Human-Machine Interface (HMI).

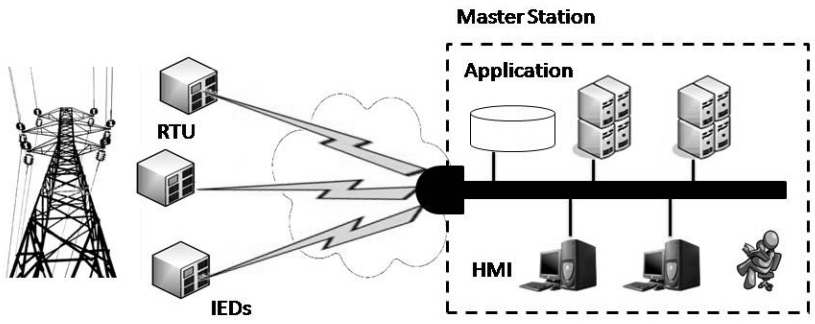

Fig. 1. Conventional SCADA Architecture

Data acquisition begins at the RTU, IED (Intelligent Electronic Device) or PLC level and includes meter readings and equipment status reports that are communicated to SCADA as required. Data is then compiled and formatted in such a way that a control room operator using the HMI can make supervisory decisions to adjust or override normal RTU (PLC) controls. Data may also be fed to a Historian, often built on a commodity Database Management System, to allow trending and other analytical auditing [5].

Recently, OLE for Process Control (OPC) has become a widely accepted solution for intercommunicating different hardware and software, allowing communication even between devices originally not intended to be part of an industrial network. Central computer of the data acquisition system, located in the hydro power plant, provides measurements performance according to a preset program, the instrumentation existing at this time and remote communications by RS485 bus, using Master-Slave architecture and IEC1107, Modbus RTU, ASCII protocols [7].

3 Wireless SCADA Communications

SCADA systems are composed of four major components: the master station or the central controller, plc/rtu/ied (deployed in remote stations), fieldbus and sensors. In Fig. 2, the architecture of SCADA system that replaces the fieldbus with wireless communication. Along with the fieldbus, this setup is extended to the Internet. This setup is similar with a private network so that only the central controller can have access to the remote assets. The central controller also has an extension that acts as a web server so that the SCADA users and customers can access the data through the SCADA provider website [8].

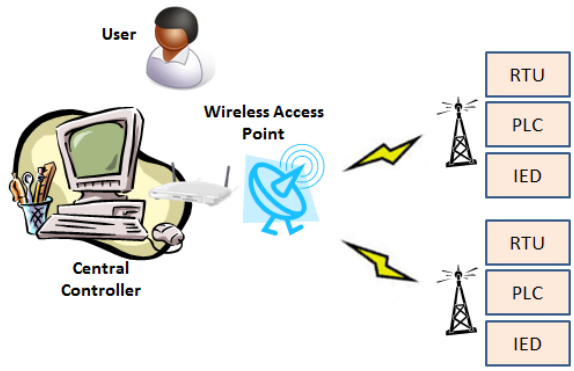

Fig. 2. Wireless Communication for SCADA systems

AS the system evolves, SCADA systems are coming in line with standard networking technologies. Ethernet and TCP/IP based protocols are replacing the older proprietary standards. Although certain characteristics of frame-based network communication technology (determinism, synchronization, protocol selection,

environment suitability) have restricted the adoption of Ethernet in a few specialized applications, the vast majority of markets have accepted Ethernet networks for HMI/SCADA.

A few vendors have begun offering application specific SCADA systems hosted on remote platforms over the Internet. This removes the need to install and commission systems at the end-user's facility and takes advantage of security features already available in Internet technology, VPNs and SSL. Some concerns include security [9], Internet connection reliability, and latency.

4 Conclusion

Wireless communications for SCADA systems is a practical solution and is required for applications when wired or line communications to the remotely deployed units is prohibitively expensive or it is too time consuming to construct. It can replace or extend the fieldbus to the internet and reduce the cost of installation. This paper presents wireless communication architecture for SCADA systems.

References

1. http://en.wikipedia.org/wiki/SCADA.
2. Hildick-Smith, Andrew, “Security for Critical Infrastructure SCADA Systems,” (SANS Reading Room, GSEC Practical Assignment, Version 1.4c, Option 1, February 2005), http://www.sans.org/reading_room/whitepapers/warfare/1644.php
3. http://www.dpstele.com/dpsnews/techinfo/scada/scada_communication.php
4. Reed, T. At the Abyss: An Insider’s History of the Cold War. Presidio Press, March 2004.
5. Tai-hoon Kim, (2010), "Weather Condition Double Checking in Internet SCADA Environment", WSEAS TRANSACTIONS on SYSTEMS and CONTROL, Issue 8, Volume 5, August 2010, ISSN: 1991-8763, pp. 623
6. D. Bailey and E. Wright, Practical SCADA for Industry, 2003
7. COSTIN CEPISCA, HORIA ANDREI, EMIL PETRESCU, CRISTIAN PIRVU, CAMELIA PETRESCU, "Remote Data Acquisition System for Hydro Power Plants", Proceedings of the 6th WSEAS International Conference on Power Systems, Lisbon, Portugal, September 22-24, 2006, pp. 59-64
8. Rosslin John Robles, Kum-Taek Seo, Tai-hoon Kim, "Communication Security solution for internet SCADA", Korean Institute of Information Technology 2010 IT Convergence Technology - Summer workshops and Conference Proceedings, 2010.5, pp. 461-463
9. D. Wallace, (2003), "Control Engineering. How to put SCADA on the Internet", http://www.controleng.com/article/CA321065.html [January 2010]