

©2008 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

Security Issues and Quality of Service in Real Time Wireless PLC/SCADA Process Control Systems

Halit Eren and Dincer Hatipoglu

Curtin University of Technology
Department of Electrical and Computer Engineering
Kent Street, Bentley, WA, 6102, AUSTRALIA

Tel: 61-8-9266 7903, Fax: 61-8-9266 2584, e-mail: h.eren@exchange.curtin.edu.au

Abstract – A wireless PLC/SCADA network has been set up to investigate the reliability of wireless communication systems in a local area network. It has been shown that the integrity of data flow can be maintained within certain limits of the signal strength in a coverage area of an Access Point. The Wi-Fi can successfully be applied in industrial operations provided a careful site surveys has been conducted and the boundaries are determined to ensure adequate signal strength to avoid any possible dropouts however short lived they may be. It has also been shown that if the dropout occurs the self repair capability of the communication system may not be sufficient thus requiring manual interference that may not be tolerable in many process control operations.

Keywords – wireless instruments, wireless sensor networks, process control, SCADA, PLC, Wi-Fi, data security.

I. INTRODUCTION

In many industrial operations, sensors and actuators are networked through Programmable Logic Controllers (PLCs) as they play important role in monitoring and controlling operations. Today there are different types of PLCs with different capacity and functionality. The modern PLCs are capable to communicate with other PLCs and devices since they usually are equipped with communications ports such as the RS232, RS485, and Ethernet. Various fieldbuses such as Modbus, DeviceNet or Profibus can be used as communication tools. PLCs are capable of controlling a wide range of sensors and output devices and have ability to incorporate and transfer real data to the system [1], [2]. Because of many advantages the PLCs are one of the most widely used devices in industrial control system.

Most PLC control systems are based on wired communication networks. Nevertheless, many industrial organizations are willing to use a wireless networks for monitoring and controlling. This prompts issues relating to the integration of older and newer technologies while the new technologies are implemented, along with the sensitivity to system quality and reliability factors associated with the transmission of information in wireless media [3], [4]. This paper investigates some safety and reliability aspects in the applications of wireless networks in industrial operations.

In addition PLC technology, Supervisory Control and Data Acquisition (SCADA) systems are used in modern industrial operations. SCADA is a term adopted by the process control industry to describe a collection of computers, sensors and other equipment suitably interfaced in order to monitor and control processes. Traditionally, remote control operations are achieved by the use of telemetry, which is a technology that gathers and sends information from and to remote locations from a central station by radio frequency communication devices [5].

The purpose of the central control station is to gather data from various Remote Terminal Units (RTUs) and provide a Human Machine Interface (HMI). Operators, at the central stations are familiar with HMI software for the display of information coming from the sensors and transducers and other field device and they control of the process by using HMI. The HMI interface computers are connected to Local Area Network – LAN, some of the recent developed SCADA applications support Nowadays SCADA is very sophisticated that Web interface HMI stations make process control observable through the Internet [6]. SCADA system supports more than one Master station, which provides redundancy in case of any problems associated with a master station. Database servers are also implemented to store the information gathered from the field devices. **Figure 1** illustrates the component of a SCADA system.

II. THE COMMUNICATION STRATEGY

In this paper, a wireless network containing 20 PLC/SCADA systems has been configured as a Local Area Network, LAN. The PLCs and SCADA set up has been based on the Factory Intelligent Network Services (FINS) Gateway (termed as FinsGateway) for communication purposes. FinsGateway is a powerful technique for factory automation FINS commands allow different types of instructions to be passed from one network type to another, regardless of the protocol type used on the network. This enables intercommunication capabilities across multiple networks and makes the controlling or monitoring of the PLCs possible from different network types. FINS Commands are defined in the application level and do not depend on lower levels (i.e. the physical and data link

levels) hence can be used across a variety of networks and CPU buses, specifically with Ethernet, Controller Link, and Host Link networks, and between CPU Units and CPU Bus Units [8], [9].

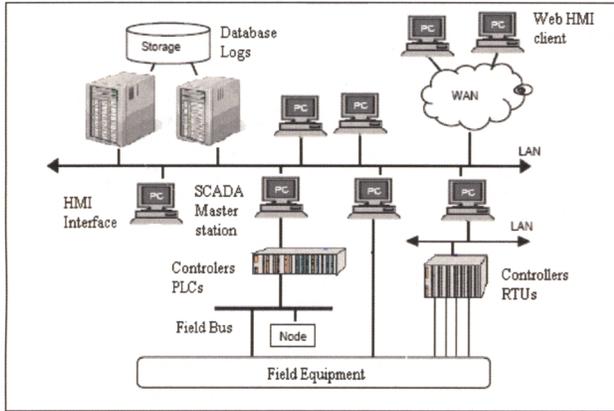


Figure 1 SCADA System hardware components [7]

Apart from the local communications between PLCs and SCADA, it was important to select a communication system that could be used to monitor and control the PLCs remotely. Different wireless technologies were investigated and in order to find the most suitable technology, the selection was done based on the following criteria:

- Bandwidth
- Range
- Security
- Speed

The bandwidth was important because the monitoring was required to take place in real time. Supervisory packages demanded high bandwidth; therefore selecting a wireless technology with higher bandwidth was an advantage. The range of communication between wireless stations was also important, as the aim was to provide flexibility and maximum distance between the wireless clients. Security on the other hand, has become an important issue in wireless communication as inadequate security poses significant disruption risk in industry processes that use wireless communication. The speed was important since the network was relatively large and demanding continuous information flow between the devices that are geographically distributed.

The most suitable wireless technology that would be readily available and meets the all the above criteria considered to be the 802.11 Wi-Fi. The Wi-Fi is an IEEE 802 protocol that expands the Open Systems Interconnection (OSI) reference model at the physical and Data Link Layer (DLL). The DLL layer consists of two additional sublayers: Logical Link Control (LLC) and Media Access Control. The LLC sublayer controls data link communication and defines the use of the logical interface points. The MAC sublayer provides shared

access of multiple devices in the physical layer. MAC directly communicates with Network Interface Cards (NICs) and is responsible for ensuring error free data communication between the network and NICs. The role of the physical layer 802.11 is to handle the transmission of data between nodes. In the LAN systems, the signal is modulated using spread spectrum, which is a technique that generates and expands bandwidth signal [10], [11].

In this study special attention was paid for network security as there are devices in the marketplace offering different levels and types of security. The security in 802.11 protocol family is defined by 802.11i protocol. In early years of implementation of 802.11 protocol, where the security was not an issue the data have been encrypted by using a Wired Equivalent Privacy (WEP) algorithm. The data exchanged between wireless stations is ciphered with a 40 or 128 bit WEP encryption key. The WEP algorithm, however, attempts to serve as both authentication and a privacy mechanism [12]. In order to address the issue of weak security, the Wi-Fi Alliance announced specification to improve Authentication Framework called Wi-Fi Protected Access (WPA), which is based on 802.11i protocol and is intended to improve the security by increasing the size of the keys and the Initialization Vector, thereby reducing the number of packets sent with related keys, and adding a secure message verification system. In order to improve the Authentication Algorithm WPA introduced Extensible Authentication Protocol (EAP), which supports EAP-Transport Layer Security (EAP-TLS). To incorporate the new advanced security measures the users authenticate to a RADIUS (Remote Authentication Dial in User Service) server [12], [13], [14].

III. SYSTEM IMPLEMENTATION

The wireless PLC network was supported by Cisco Aironet 1200 system. The network was distributed in various rooms in a building as shown in Figure 2.

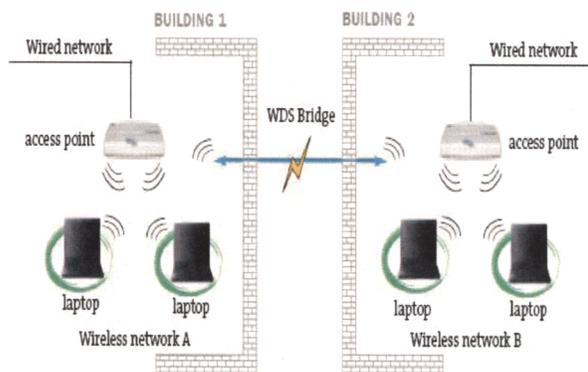


Figure 2 Experimental wireless network topology

The Cisco Aironet 1200 system could function as an access point or bridge whether set as a single-band or dual-band platform, allowing each radio to be individually configured as an access point repeater, root bridge, non-root bridge or workgroup bridge, enabling a broad array of applications [15]. The access point has unified IDS/IPS features enabled for the wireless security.

The management frame protection of the Cisco Aironet 1200 was part of its infrastructure, which allows the network to detect spoofed frames from access points or malicious users impersonating infrastructure access points. If an access point detects a malicious attack, an incident will be generated by the access points and reports will be gathered on the Cisco wireless LAN controller, Cisco WCS, or CiscoWorks WLSE. The Access point has hardware-Assisted AES Encryption, which provides high security without performance degradation. Also, the access point is IEEE 802.11 i-Compliant; WPA2-Certified and WPA-Certified, which helps to ensure interoperable security with wireless LAN client devices from other manufacturers [16].

During the experiment the Cisco Aironet 1200 was configured by HyperTerminal. A RS-232 serial cable was connected between the access point's configuration port and a com port of the PC terminal. The configuration of the HyperTerminal is shown in Table 1.

Bound rate	9600
Data Bits	8
Parity	No parity
Stop Bit	1
Flow Control	Xon/Xoff

Table 1 Configuration settings of the HyperTerminal

After completion of the PLC, SCADA and Wireless Network implementation, the system was integrated and ready to run the simulation of a Car Washing Process. The simulation could be operated by the PLC as well as from the control buttons on the HMI terminal. The PLCs were connected to the access point via a network hub. The access point and the wireless station communicated wirelessly at 11 MB using IEEE802.11 protocol. The screen shots of CWS simulation is shown in Figure 3, which illustrates four different processes of the car washing: spraying the soapy water, rinsing with water, drying and moving the car out from the base station.

During the monitoring it was important that the integrity of data was maintained. Therefore information flow from the tags of the SCADA has been monitored continuously by exporting them into an EXCEL files as shown in Figure 4. For this, Object Linking and Embedding (OLE) for Process Control (OPC) client software have been configured. OPC is a new technology designed to bridge Windows based applications and process control hardware. It is an open standard that

is used to access field data from plant floor devices. The OPC client used during the data integrity checking was from the Matrikon OPC [17]

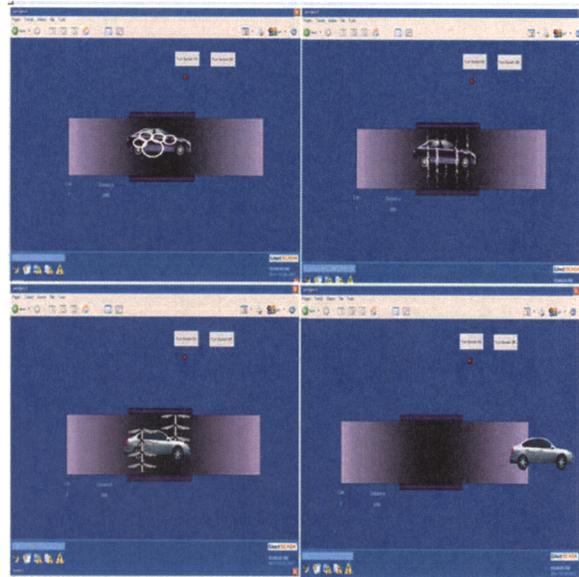


Figure 3 Screenshot of SCADA/HMI appearances

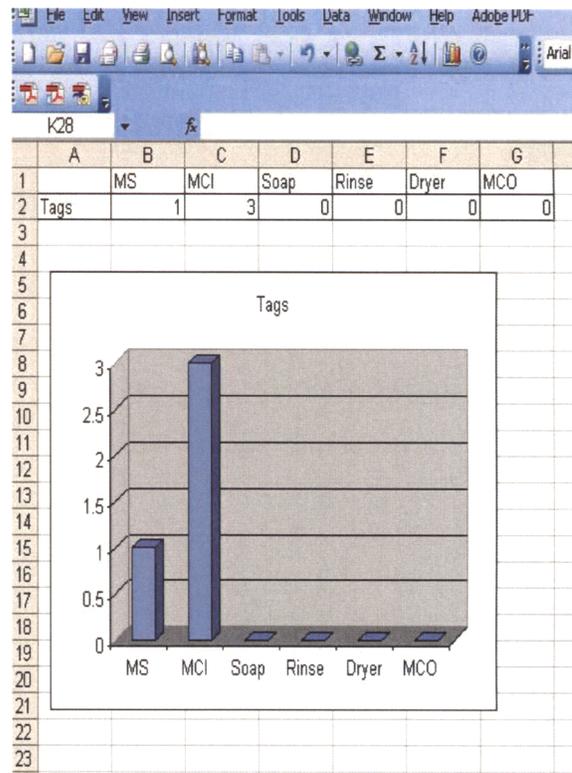


Figure 4 Monitoring of the tags from EXCEL output file

Figure 4 Monitoring of the tags from EXCEL output file

The information flow from the tags of the SCADA were gathered in the form of EXCEL files for the following cases:

- PLC 10m apart from the Access Point
- PLC 30m apart from the Access Point
- PLC 50m apart from the Access Point

Many experiments were conducted for testing of reliable and continuous operations. A typical connection historical data has been shown in Figure 5.

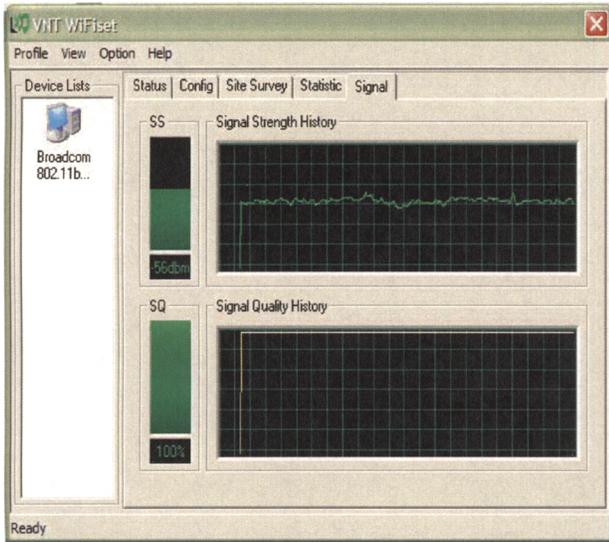


Figure 5 Wi-Fi set of serial-wireless access point

When the distance between the Access point and the wireless client was 10m the signal strength was measured as 92% with the response time of 2ms, shown in Figure 6.

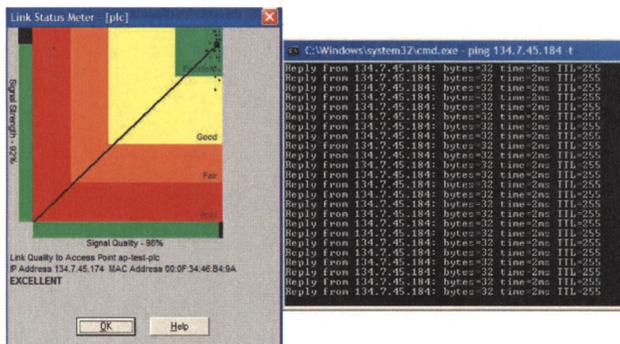


Figure 6 Signal strength and response time from 10m

When the distance between the Access point and the wireless client was 30m the signal strength was measured as 55% with the response time of 18ms, shown in Figure 7.

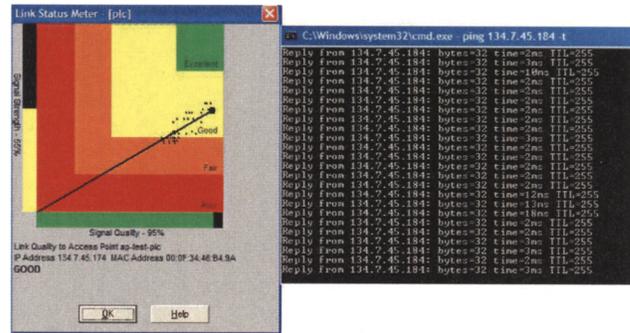


Figure 7 Signal strength and response time from 30m

When the distance between the Access point and the wireless client was 50m the signal strength was measured as with an inconsistent the response time. It was noted that after 600ms response time the connection dropped, shown in Figure 8.

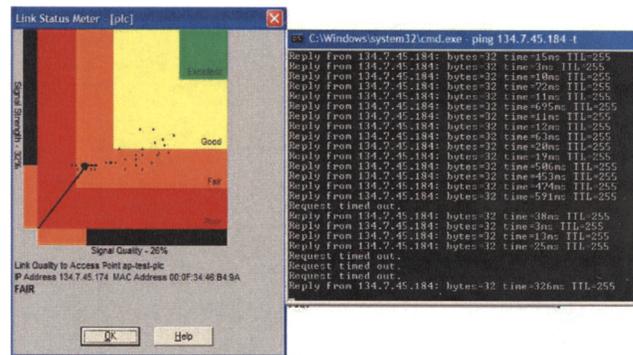


Figure 8 Signal strength and response time from 50m

When the connection has dropped out, the tags in the output file did not match the tags results of the base file. When the laptop was moved few meters towards the Access Point, the wireless connectivity was re-established and PLC responded. However, after the re-establishing connectivity the simulation did not run without re-initializing the FinsGateway services. When the error on the FinsGateway was cleared the application restarted. Restoring the FinsGateway services was about 30s, which may be regarded to be unacceptable in many industrial applications that require continuous operations.

These results have shown that although transmission power of Wi-Fi can be improved by the use of suitable antennae if the power is already set there is a limit in the operations before a dropout occurs. Unlike many wireless sensor networks where dropout and network recovery are tolerated by the design, clearly dropout may not be permissible in large networks that require continuous operations. Process control is a typical example of the systems that require continuous operations for safety reasons, emergency, and inherent dataflow requirements between sensors and control devices. This is particularly important in processes where continuous feed-

back systems are involved. This work is expanded to close feedback control systems that are integrated with wireless communication networks.

- [16] Cisco <http://www.cisco.com> accessed 10/10/2007
[17] Matrikonopc, <http://www.matrikonopc.com> , accessed 10/10/2007.

V. CONCLUSIONS

In this study it has been shown that the Wi-Fi can be used for wireless operation of PLC/SCADA process control systems. Given the transmission power of the wireless system, the data integrity of dataflow can be maintained while the signal strength between the wireless client and the Access Point is maintained at the level above 45% with response delay no more than 600ms. For successful applications of Wi-Fi in process control industry site surveys should be conducted to determine the boundaries of the coverage area where there is sufficient signal strength. The coverage area can also be extended by installing a second Access Point where coverage areas overlap with the first Access Point.

REFERENCES

- [1] Balakirsky, V.B. and Han Vinck, A.J. "Potential performance of PLC systems composed of several communication links," *International Symposium on Power Line Communications and Its Applications*, Vancouver, BC, Canada, pp.12-16, 2005.
- [2] Kaneyama, T., Mineno, H.; Furumura, T.; Yamada, K.; and Mizuno, T. "Reliable communication methods for mutual complementary networks," *Knowledge-Based Intelligent Information and Engineering Systems. 10th International Conference, KES 2006. Proceedings, Part III*, pp. 150-8, Bournemouth, UK, 2006.
- [3] Almeida, J.A. and Fernandes, J.M., "Industrial automation and communication," *ISA TECH/EXPO Technology Update Conference Proceedings*, Houston, TX, Vol. 416, pp. 237-246, 2001.
- [4] Zezulka, F., Bradac, Z.; and Kucera, P., "Formal methods for higher reliability of the industrial automation," *IEEE International Conference on Industrial Technology*, Maribor Slovenia, Vol. 2, pp. 891-5, 2003
- [5] Williams, A., "PC SCADA takes control? Will the PLC be killed by SCADA based soft logic controllers?" *Bi-Annual Symposium and Exhibition. SCADA towards 2001. Proceedings*, Gatwick, UK, pp. 15, 1997.
- [6] Mintchell, Gary A., "HMI/SCADA software more than pretty pictures," *Control Engineering*, v 49, pp. 18-25, 2002.
- [7] D. Bailey, *Practical SCADA for Industry*, Newnes, 2003.
- [8] Omron, "Communications Commands, Reference Manual, SYSMAC CJ Series," 2006.
- [9] Xu Shi-xu; Zheng Jian; and Sun Wei-guo, "The monitor system design of controller link based on VC" *Journal of Qingdao University of Science and Technology (Natural Science Edition)*, Vol. 22, No. 1, pp. 30-4, 2007.
- [10] Eren, H., *Wireless Sensors and Instruments - Networks, Design, and Applications*, CRC-Press, Boca Raton, USA, 2006.
- [11] Brown, S., "Scalable wireless data networks," *Elektronik Praxis*, No. 17, pp. 24-6, 2005.
- [12] M. Gast, *802.11 Wireless Networks*: O'reilly, 2002
- [13] Chendeab, N., El Hassan, B., and Afifi, H., "Performance evaluation of the security in wireless local area networks (Wi-Fi)," *Proceedings - 2004 International Conference on Information and Communication Technologies: From Theory to Applications, ICTTA 2004*, Damascus, Syria, pp. 215-216, 2004.
- [14] Accomando, R., "Security in wireless networks," *Elettronica Oggi*, Vol. 350, pp. 78-80, 2005.
- [15] Molta, D., "Flying on Aironet [wireless LAN]," *Network Computing*, Vol. 13, No. 23, pp. 27-8, 2002.