RESEARCH ARTICLE OPEN ACCESS

Study on Optimizing Industrial Wireless Network Performance

Seema Sinha [1], Dr. Deva Prakash [2], Manish Kumar [3]
Research Scholar [1], University Dept. of Mathematics, Magadh University, BodhGaya
Associate Professor [2], Dept. of Mathematics, S.M.D. College, Punpun
Research Scholar [3], University Dept. of Mathematics, Magadh University, BodhGaya
Bihar - India

ABSTRACT
This paper reveals that the performance of wireless networks can change over time due to increased performance demands, changes in the radio frequency (RF) environment and changes in the physical environment. This article will explore the use of a wireless diagnostic OLE for Process Control (OPC) server technology to embed diagnostic information in human machine interfaces (HMIs), thus optimizing industrial wireless network performance.

Keywords:- Radio Frequency, OLE for Process Control, SCADA Network, Automatic Guided Vehicle

I. INTRODUCTION

Wireless communications is becoming increasingly popular for factory and process control automation systems. Part of this growth is due to the emergence of very reliable radio frequency technologies capable of handling the extreme conditions present in industrial plants. The other factor driving growth is the realized benefits that wireless presents including reduced installation costs, elimination of phone line charges for remote sites, reduced mechanical wear to moving platforms (thus improving performance of material handling systems) and providing crucial information for production and maintenance workers wherever needed.

The acceptance of wireless strategies to reduce costs and improve productivity has lead to wireless being relied upon in many crucial processes. As more systems become dependent on wireless networks, it is important to include intelligent diagnostics to detect network degradation and prevent communication failures before they occur. Changing conditions are a given in most plants, however, those changes can affect wireless performance. Therefore the continuous monitoring of the RF network is good practice and can eliminate unexpected shut downs.

Diagnostic techniques vary greatly by industrial wireless manufacturer. There are some “industrial” wireless devices that do not include any diagnostic information at all. Either the data is received correctly or not. These are understandably very difficult to troubleshoot when problems are encountered. Other systems provide offline diagnostics where communication must be stopped in order to access the diagnostic information. These systems at least provide some insight into the cause, but only after the failure has occurred.

Online wireless diagnostics provide continuous monitoring of wireless performance and hardware conditions of the entire wireless system, local and remote. These tools can not only detect a failure, but show degrading conditions as well. Because the diagnostic metrics are being monitored in real time, there is no need to shut communications down to check the system. However, there is no free lunch! Because the diagnostic data travels over the same wireless link as the system data, performance can degrade when diagnostics are active. In systems with a large number of remotes and high

amounts of data transfer, online diagnostics may be impractical.

The methods to access online diagnostic information vary by manufacturer and wireless system. Some wireless serial systems use a second serial port and communication is done using a menu-driven interface accessible from a dumb terminal program (such as a HyperTerminal). Other online diagnostic systems use a proprietary software program where the PC attaches to either the secondary serial port or is part of the Ethernet network, and displays vital information about the RF network using a proprietary software program. Still other systems (commonly 802.11 based) have embedded web servers for diagnostic information. The diagnostic information is then displayed using a web browser. In Ethernet-based wireless networks, potentially anyone on the Ethernet network can view the diagnostic pages of local and remote wireless equipment.

What the previously described methods lack is the ability to easily integrate diagnostic status and information directly into the control system. They are especially burdensome for plant operators that lack computer skills and technical aptitude. For example, expecting a third shift operator in a wastewater plant to understand the vendor’s diagnostic program (or diagnostic web page) and diagnose the problem is probably expecting too much. Therefore it is highly desirable to have a method for remote RF diagnostics where the control engineer can appropriately embed diagnostic data.

SNMP (Simple Network Management Protocol) is one possible way to access diagnostic information in a common approach. SNMP is a standard diagnostic language developed primarily for the management of information technology devices.[1] SNMP provides a way for diagnostic software tools to manage and monitor devices manufactured by different vendors. While a few industrial devices now include SNMP support, most industrial software programs do not. Therefore SNMP-based management tools are not very practical for industrial wireless systems.

Integrating Diagnostics

This leads us to consider what the best method is for integrating wireless diagnostic into industrial systems. OPC (OLE for Process Control) is likely the best approach as it is a software data exchange standard developed specifically for industrial systems, and is widely deployed and supported. Using OPC as the basis for RF diagnostics provides any OPC compliant software programs (such as most major HMI and SCADA software packages) direct access to the diagnostic information. And because control engineers are well versed in developing projects using these programs, wireless diagnostic data is easily included in operator interfaces just like any other tag data point.

Using an OPC server for wireless diagnostics opens up many possibilities for monitoring and optimizing the wireless network. To fully understand the possibilities, it is first useful to examine the key diagnostic metrics that are often monitored. In RF systems, links are established between wireless devices (sometimes known as wireless access points, bridges and clients) using pre-determined RF channels and authentication routines. Each wireless device both transmits and receives (but not at the same time). When an RF signal is transmitted, it has certain amount of energy (measured in dBm, or decibels below one milliwatt). Loss occurs through the air based upon distance and if obstructions are in the way. When the signal is received at the remote antenna, the signal must be strong enough for successful data transmission. The strength of the received signal is known as RSSI (Received Signal Strength Indicator).[2]

Another very important measurement is the noise within the channel. The received signal must be higher than the noise in the band to decode the information. Noise is also measured in dBm. We'll discuss noise and its causes later in this article.

Another common metric is signal-to-noise ratio which is calculated using measured signal strength (RSSI) and noise. The higher the ratio, the more reliable the system will operate.[3]

As data packets are exchanged, most industrial wireless devices will include an error correction algorithm to ensure that packets are received successfully and retransmitted if necessary. Diagnostic tools can report the number of packets successfully transmitted and the number of bad packets received. This provides a way to calculate RF error rates, which is another key metric.

Diagnostics can also monitor the number of attached nodes (clients). This metric is interesting because it can quickly report (alarm) if a link goes down *and* also report if the number of attached clients is *higher* than expected thus representing a possible security threat.[4] It is also possible to monitor the identity (MAC address) of the attached wireless clients, adding additional security.

Finally the number of bytes transmitted is a useful measurement because it shows actual utilization of the wireless link.[5] By calculating bytes transmitted per second and comparing it to the capacity of wireless technology, bandwidth utilization is monitored.

Wireless diagnostics can include many other attributes, but these are considered the essential ones. Other metrics that may be monitored include environmental conditions (temperature, supply voltage), VSWR (Voltage Standing Wave Ratio) useful for detecting antenna or coax problems and channel frequency drift.

II. COMMON WIRELESS DIAGNOSTIC METRICS

Metric	Description	Diagnostic Use
Signal Strength (RSSI)	**Measures the strength of the incoming RF signal. Typically measured in dBm**	*Key measurement for link quality. Link will fail or provide intermittent communications if below the receive threshold of the RF receiver. Possible causes include radio, antenna, coax cable problems or obstructions between antennas.*
Noise Level	**Measures the interference level present in the RF channel of use. Typically measured in dBm.**	*Another key measurement for link quality. If noise is too high, the link can degrade or fail. Possible causes include saturation of the band from other RF systems, improper antenna cable grounding, harmonics from electrical equipment*

		or radio hardware problems.
Signal-to-Noise Ratio (SNR)	**The margin between signal strength and measured noise. Typically measured in dB.**	*Signal strength should always be higher than noise level for reliable communications. It is good practice to maintain a signal strength at least 10 dB higher than noise. To improve SNR, either increase signal strength (e.g. higher gain antennas) and/or lower noise levels (e.g. use a different channel or use directional antennas).*
RF Packet Errors	**The number of wireless packets received in error.**	*In systems using Cyclical Redundancy Checking (CRC) error correction as opposed to Forward Error Correction, every packet that is received in error must be re-transmitted thus reducing data throughput and slowing performance. Packet errors may be due to weak signal strength and/or high noise levels.*
Data Bytes Received	**The amount of data successfully received.**	*Efficient data exchange between devices is the function of a properly operating wireless network. Measuring the number of data bytes received at each node reveals link quality and utilization. Slow data reception may be due to high RF packet error rate and poor link quality. Additionally, link utilization may be calculated by measuring bytes received over time and comparing to the capacity of the RF system.*
RF Connections	**Number of wireless devices connected to an access point or repeater.**	*This metric provides insight into the condition of the RF system and security. If the number of RF devices (clients, repeaters, other access points) is lower than expected, a communication problem exists. If the number is higher than expected, a possible security breach is detected.*
VSWR	**Voltage Standing Wave Ratio reports amount of antenna reflected power**	*Antenna systems are designed to efficiently transfer RF energy. The efficiency can be measured by monitoring reflected antenna power. If too high, then RF performance is impeded. The likely cause is degraded coax cable (e.g. corrosion of RF connectors) or loose fittings.*

III. OPERATING AN OPC-BASED DIAGNOSTIC SYSTEM

Now that we have an understanding of the metrics available for monitoring, we can explore how to implement and operate an OPC based wireless diagnostic system. First it is important to note that only one server is required to collect the diagnostic information. For Ethernet systems, wireless diagnostic OPC servers can be present anywhere on the network. They are configured to collect the designated diagnostic data for each selected wireless device.[7]

Because the server is located at one particular leg of the wireless network, the server is collecting some of the diagnostic data over the hard-wired Ethernet network and others over the wireless network. Therefore if a link fails, diagnostics are obviously lost for that particular device. It is generally good practice to locate the server where it will have the fewest number of wireless connections for the diagnostic data to transverse so if a wireless link fails, the critical OPC clients have access to the server. *Diagram 1* illustrates how one centrally located OPC server can collect wireless diagnostic information and make it available to all HMI clients on the local and remote networks. For more complex networks, it may make sense to install more than one OPC server thus proving diagnostic information directly to more clients.[8]

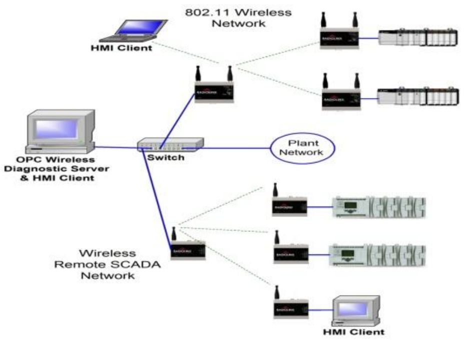


Diagram 1. The Wireless OPC Server collects diagnostic data from two separate RF networks. Any HMI client on the logical network has access to the diagnostic information.

Once the server is installed, it will routinely poll the designated diagnostic data from each wireless device. The frequency of the poll is usually configurable and could be as quick as every 100 ms or as slow as every 60 seconds. This setting is dependent upon how vital the current information is to the application and how congested the wireless network is.[9] The quicker the update time, the more wireless bandwidth is being used for diagnostics, and the less available for the application.

The server will usually organize the diagnostic data by device name (or other user designation) and each metric will become a unique tag for the OPC client. Most HMI and SCADA software packages are OPC compliant and provide a way to browse for available OPC tags. Once the tags are detected by the client, they can be used in virtually any way that the control engineer requires.[10]

Before developing the project, consider the overall communication architecture of the system. Where are the vital links? What would happen if a link fails? How can I prevent a problem before it occurs?

Once the network architecture is understood, consider the needs of each user. A production worker probably has no idea what RSSI means, but could convey to the supervisor if the HMI is stating that a wireless link has failed. If the operator is alone, the HMI could advise who to contact (e.g. SI responsible for the wireless link, or engineer on call if a PLC problem). The operator also has a way to know that the wireless link is functioning, so if a system problem occurs, the fault is not in communications.[11] Conversely, the engineering manager may want to view all relevant data on a screen monitoring the entire wireless network. The more detail, the better because the engineer could decipher the meaning of each. It is important to tailor the HMI display for the skill sets and knowledge of the user.

Most HMI and SCADA software packages also support alarming and trending functions. Alarms can notify the operator, maintenance manager or engineering manager of a fault condition (like a wireless link failure) or if communications are degrading so that preventative action can be scheduled. Alarms can also be sent remotely (like an email over the Internet, or cell phone text message) so that notification is immediate.

Trending functions are useful for reviewing performance history and analyzing correlation. For example, the number of bytes transmitted can be trended over time to see if throughput demands are increasing.

It is also possible for automation equipment (such as PLCs) to access OPC data within their internal program.[12] This opens up the possibility of not only notifying operators/managers when a problem occurs, but having the PLC program act on it. For example, if a wireless link fails then the PLC could activate a back-up communication link (such as a redundant wireless connection). In this case, the system would recover without any human intervention.

As you can see, there are many ways to use RF diagnostic data when made available in an OPC server. The best use is dependent on the process type, how wireless is being used in the system and user needs. Here are a few example applications.

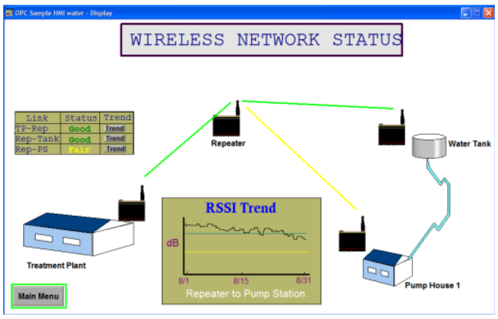
Application 1 – Wastewater Pump Stations

A wastewater facility uses a wireless SCADA network to connect several remote pump stations. The water treatment plant PLC remotely turns on and off the pumps based on flow measurements. Each RF link is several miles, so travel to a pump station takes time.[13]

The system integrator has decided to use OPC-based wireless diagnostics in the following ways:

- Operator interface notification of link failure
- Alarm notification sent to plant superintendent
- Trending of RSSI to monitor change in line-of-sight (e.g. tree growth)

The operator interface displays RF Links Status between the Pump Station and Water Treatment Plant. If a pump station is not starting (for example), the operator could quickly tell if the link is at fault. If not, then there is another problem and the operator can contact the appropriate person or travel to the site to repair the problem.

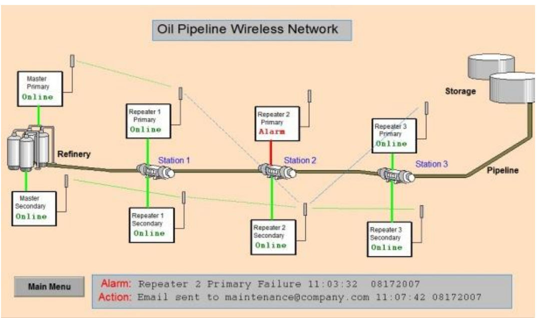


Application 2 – Oil Pipeline

An oil distribution system uses a wireless SCADA network for pipeline flow measurement, leak detection and valve actuation. The pipeline is many miles long using wireless Ethernet repeaters to span the entire length. The SCADA network provides automatic process control via a PLC system. Operators may monitor alarms and manually control valves, while the system collects oil flow data.

Because the SCADA network is critical for the pipeline operation, the system uses redundant repeaters using mesh network architecture.[14] That way if a repeater fails due to a hardware failure or damage from an electrical storm, communications are not lost.

Using OPC tags, the HMI displays and monitors the RF conditions between each repeater site. The system quickly detects if a repeater site has failed or is close to failing. If a failure occurs, the RF system automatically heals itself, and the operator is notified that a site has failed so that repairs may be made to reestablish the RF network redundancy. The control system may be made aware that the RF redundancy has been temporarily lost to prepare for a safe shutdown in case communications are lost.

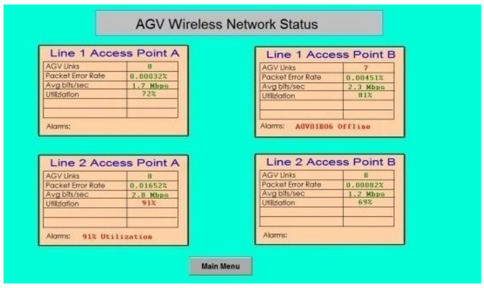


Application 3 – Automotive AGV System

An automotive assembly plant uses an automatic skid system to transport assemblies through out the assembly process. Each AGV (automatic guided vehicle) uses an RF link to synchronize its movement and tooling with the rest of the system. The wireless Ethernet system is used to link EtherNet/IP remote I/O to a PLC system. Because of the high I/O count and fast scan rates, the Ethernet data traffic is very high. It is critical that the wireless network provides high data throughput and does not drop packets.

In this system, the OPC diagnostic server is configured to sample RF conditions only once every minute. This ensures that the diagnostic data collection has limited impact on data throughput.

In addition to monitoring the health of the RF network, the operator interface will monitor the number of connected clients per access point. If the number is below what is expected, then a skid has dropped offline and an alarm is set. The system also reports data rate to each client. If the data rate is close to the capacity of the wireless technology, then the PLC will bring online an alternate link while setting an alarm. The engineering staff can then determine if traffic over the RF network is rising because of inappropriate traffic (data flowing over the network that is not for this process) or changes to the program.



IV. CONCLUSION

On the basis of above analysis, the present paper concludes that the performance of wireless networks can change over time due to increased performance demands, changes in the radio frequency (RF) environment and changes in the physical environment. Diagnostic techniques vary greatly by industrial wireless manufacturer. There are some "industrial" wireless devices that do not include any diagnostic information at all. Either the data is received correctly or not. These are understandably very difficult to troubleshoot when problems are encountered.

REFERENCES

[1] Dai H.N. Throughput and delay in wireless sensor networks using directional antennas; Proceedings of the 5th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP2009); Melbourne, Australia. 7–10 December 2009; pp. 421–426.

[2] Pradhan N., Saadawi T. Energy efficient distributed power management algorithm with directional antenna for wireless sensor networks; Proceedings of the 34th IEEE

Sarnoff Symposium; Princeton, NJ, USA. 3–4 May 2011; pp. 1–6.

[3] Lakshmanan S., Tsao C.L., Sivakumar R., Sundaresan K. Securing wireless data networks against eavesdropping using smart antennas; Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS'08); Beijing, China. 17–20 June 2008; pp. 19–27.

[4] Shiu Y.S., Chang S.Y., Wu H.C., Huang S.C.H., Chen H.H. Physical layer security in wireless networks: A tutorial. IEEE Wirel. Commun. 2011;18:66–74. doi: 10.1109/MWC.2011.5751298.

[5] Patwari N., Ash J.N., Kyperountas S., Hero A.O., Moses R.L., Correal N.S. Locating the nodes: Cooperative localization in wireless sensor network. IEEE Signal Process. Mag. 2005;22:54–69. doi: 10.1109/MSP.2005.1458287.

[6] Dai H.N., Ng K.W., Li M., Wu M.Y. An overview of using directional antennas in wireless networks. Int. J. Commun. Syst. 2013;26:413–448. doi: 10.1002/dac.1348.

[7] Godara L.C. Smart Antennas. CRC Press; Boca Raton, FL, USA: 2004.

[8] Chong N.K., Leong O.K., Hoole P.R.P., Gunawan E. Smart Antennas: Mobile Station Antenna Beamforming. In: Hoole P.R.P., editor. Smart Antennas and Signal Processing. WIT Press; Southampton, UK: 2001. pp. 245–267.

[9] Nowicki D., Roumeliotos J. Smart Antenna Strategies. Mob. Commun. Int. 1995;4:53–56.

[10] Balanis C.A. Modern Antenna Handbook. John Wiley & Sons; New York, NY, USA: 2008.

[11] Allen B., Ghavami M. Adaptive Array Systems: Fundamentals and Applications. John Wiley & Sons; Chichester, UK: 2005.

[12] Ahmad A., Ahmad S., Rehmani M.H., Hassan N.U. A survey on radio resource allocation in cognitive radio sensor networks. IEEE Commun. Surv. Tutor. 2015;17:888–917. doi: 10.1109/COMST.2015.2401597.

[13] Elkashlan M., Duong T.Q., Chen H.H. Millimeter-wave communications for 5G: Fundamentals: Part I (Guest Editorial) IEEE Commun. Mag. 2014;52:52–54. doi: 10.1109/MCOM.2014.6894452.

[14] Roh W., Seol J., Park J., Lee B., Lee J., Kim Y., Cho J., Cheun K., Aryanfar F. Millimeter-Wave beamforming as an enabling technology for 5G cellular communications: Theoretical feasibility and prototype results. IEEE Commun. Mag. 2014;52:106–113. doi: 10.1109/MCOM.2014.6736750.