

Long Range Wireless Sensors for Fixed Remote Assets

Raed H Abdallah, co-founder and CTO
vMonitor, Inc.

Introduction

Wireless Sensor is penetrating every aspect of our lives and given its numerous advantages over a wired network, wireless sensor network technology is expected to grow exponentially and gain a stronghold across industry verticals. Application ranging from military usage, warehouse and retail store monitoring, medical monitoring of patient health, environmental monitoring of natural habitats and monitoring of man-made structures. These are just few examples of wireless sensor network currently in use. Another area that is gaining lot of traction in the Wireless Network world is in the Oil & Gas Industry. Monitoring and control of Remote Fixed Asset such as Well Head monitoring, Pipeline monitoring, Tank Level monitoring offer and others unique challenges not encountered in other application and there are several hardware and firmware design consideration that need to be taken into account. Low Power consumption, RF Range of the Wireless Sensors (0 to 40 miles), Path Loss Analysis, security, remote configuration and Optimal Gateway design are key factors in successful Wireless network solution.

Wireless Sensor Network

A wireless sensor network is a collection of RF wireless sensors/nodes (see Figure 1.0) collaborating and communicating by means of wireless transmission. Typically there will be at least one network gateway (access point to the network). A gateway is the heart of the wireless network and it function can range of simply passing data from/to the nodes or much more intelligent like preventing intruders, network node time synchronization, monitoring the network for alarms (i.e. node failures) and more. Wireless Sensors can be used for data collection and reporting, alarm monitoring and object tracking. There are different types of wireless network topologies including star, linear, tree. What type of topology to use depends on the application type and the majority of remote application can be fulfilled

with a simple star network. However, it is imperative that the network wireless nodes support message relaying and mesh networking in case there is a need for a much more complicated network topology and to prevent setting up dedicated repeaters.

Security

Wireless technology uses common medium for signal transmission through the atmosphere and is defenseless to external interferences, interruptions, or abuses by other parties. This medium of communication is inherently unreliable and vulnerable to unauthorized access and security breaches. There are several potential threats associated with wireless communication:

Jamming

Jamming is when the wireless signal is interrupted due to external device generating the same frequency band used by the wireless sensors. There are two types of jamming:

1. Malicious Jamming is when other users intentionally overcrowd the frequency band and overpower other devices for the sole purpose of disrupting the wireless signal.

2. Friendly Jamming is when other legitimate devices are sharing the same frequency band.

Unfortunately malicious jamming is very difficult to prevent due to the open access of wireless communication. Friendly jamming can be reduced with:

- Proper engineering to allow different wireless networks to use the appropriate frequency band to reduce conflicts
- Controlling radio output power to prevent some networks from over powering other neighboring networks.
- Routinely scanning the frequency band should be part of the system maintenance to identify and detect any interfering signals.

Eavesdropping

Eavesdropping is the ability of unauthorized party to remotely detect, intercept and listen to the wireless signal. There are several things can be done to prevent eavesdropping:

- Use of proprietary wireless system over open

protocol systems (such as WiFi) as they offer security by obscurity.

- Data Encryption (at least 28 bit Encryption) with Random keys.
- Use of directional antennas instead of Omni antennas to reduce coverage areas

Phony Data

Phony data or bogus data is the injection of false data into the wireless network using existing or non existing wireless devices ID's. Several measures can be taken to prevent phony data. These include:

- Data encryption with random keys to prevent data duplication and the hijacking of node ID's.
- The use of unique node identifier and filter (similar to MAC filter) what Identifiers are allowed within the wireless network.
- Authentication and registration for each wireless node before it can join and start broadcasting messages within the wireless network.
- Each wireless network node should have a sequence number embedded in each message to assure data integrity and the wireless network gateway should inherently have built in measures to monitor the sequence number from each node and reject bogus data that does not carry the correct sequence number.

Obviously, there should be some tolerance to rejecting messages to guard against legitimate out of sequence message number that might take place.

- In addition routine monitoring and validating of the wireless network system traffic to assure that there are no such data being injected into the system.

Low Power Consumption

Designing low power, long range RF wireless sensors must take several areas into consideration: hardware, firmware and the use alternative power source.

Hardware Consideration

In designing Wireless Sensors for remote application the following should be taken into account:

- Use of low power industrial grade material for use in harsh environment
- Built-in Timers to allow running the hardware in low power mode (sleep mode) with less than 20 Micro Amp power consumption.
- Allow to independently shut down and power up different hardware components (i.e. Radio, sensor, digital lines, etc.)
- Allow for communication modularity so that different type of radio can be used based on allowed RF output power, allowed frequency band, data throughput requirements and transmission range.

Firmware Consideration

In the wireless sensor network on application is the same and each node should be configurable to meet the client needs and requirements. The firmware must be developed allow for maximum hardware configurability. Specifically the firmware should:

- Control when and how power is shut down to go into low power mode
- Only power the radio when we are ready to transmit data.
- Control the Radio settling time and shut down time so that the smallest required amount of time. The Radio settling time is the time required after the power is supplied to the radio before the radio can transmit data. The shut down time is the amount of time the radio needs after we transmit data.
- Control the Sensor settling time so that

SUBSCRIBE TODAY TO GET
THE LATEST NEWS ABOUT



REMOTE

Site & Equipment Management

New Products, Companies, The Industry, Research & Development and Events.

For a new subscription, or to renew your current subscription go to:

www.RemoteMagazine.com/r-sub.php

smallest required amount of time is used before the measurement is taken.

• Intelligently determine when to transmit data. Data should only be transmitted upon change and when the required scheduled transmission interval is reached. This can be done by separating the sampling rate (when data is measured) from the transmission rate (when data is sent). By separating these two tasks the firmware can sample data at a much higher rate and only transmit data when necessary. It crucial that the firmware allows the user to select what constitute a change in status. In some application a 1 percent could be very significant and other application can tolerate up to 5 percent or 10 percent change.

• Ability to report by exception whenever an alarm is triggered. There are several types of alarms that can be monitored to trigger an alarm. Most common alarms include:

Min/max alarming. When data exceeds certain data range

Percent change. When the difference between two readings exceeds the allowed specified limit. With Data Push Reporting it is imperative that the comparison is between the last reported value and the current value and not just two consecutive values. Consider the case where the allowed change is 5 percent and the comparison is done between two consecutive values. If there is a small a drift in the reading (say 1 percent) then the alarm will never be triggered and over time the change between the last reported value and the current value will far exceeds the limit but it will not be detected since the drift between two consecutive reading is only 1 percent. Comparing the last reported value to the current value will prevent this and will correctly trigger the alarm.

• Control what type of data is required and only transmit what is required by the client. For instance, if a wireless sensor is collecting raw data, engineering data, linear accumulation there is no need to transmit all these data if the client only requires engineering unit data.

• Allow for remote access and configurability so the node can be configured and controlled remotely and to minimize the need to physically going to the remote location for minor changes.

Alternative Power Source

Currently there are few options available to utilize in powering low power Wireless Sensors in remote application. These include:

1. Battery
2. Solar energy
3. Power Harvesting using Vibration or Thermal

The type of energy source to use in remote installation depends on several factors including application type, sensor power requirements, reporting frequency, RF output requirements, and control requirements. Currently, and as general rule of thumb the selected power source should be maintenance free for at least one year.

Remote Access and Configuration

For remote application it is imperative to be able to remotely access and configure the network nodes. The challenge is how to accomplish this and maintain the wireless sensor low power consumption. One approach to accomplish remote accessibility to the node and maintain low power is to utilize the network gateway with a command Mail Box feature. The network gateway is the heart of the wireless network and all communications between the network nodes and the outside world (i.e. SCADA system) must pass through the gateway. Each node within the gateway wireless network will have a command mail box located on the gateway. When there is a command to be sent to the wireless node (i.e. changing the sample rate from one minute to 10 seconds) then the gateway will hold this command in the node mail

box. When the wireless node reports to the gateway and send its data the gateway will notify the node that there are messages in the node mail box waiting to be downloaded. The node then will proceed to downloading these messages and executing the commands. Using this technique the node will maintain low power consumption and still offer remote control and configuration capabilities.

Data Reporting and Alarming

There are two types of data reporting: data poll and data push. Data Poll is on demand reporting where the wireless node only reports back when the network gateway request information from the node. Data Push is unsolicited reporting where the node reports back to the gateway on a scheduled interval or by exception. Data Polling or on demand reporting reduces over air traffic and prevents data collision and it is preferred over data push reporting. However, data poll can only be achieved if the node is continuously listening to over air messages which requires much more power consumption and reduces battery life. When using Data Push or Unsolicited data reporting it must be designed to minimize over air traffic as much as possible to prevent over

air collision and lost data. How often the node should push and report data depends on the criticality of the application and the number of nodes within the network. There are few things that can be done to reduce unnecessary over air traffic. These include:

- Reduce message size as much as possible to prevent long transmission and reception cycle.
- Create different reporting messages for different data types (raw count, engineering units, accumulation data, SQRT, pulse counts, etc.)
- Selected reporting so only the required data is reported. There is no sense of transmitting pulse count data if the data is not acquired or sending raw data when the client is only interested in scaled engineering data.
- Report by exception by separating the sampling rate (when data is collected) from the reporting rate (when data is transmitted) so that the data can be measured at much more frequent interval and only transmitted if there is a change in status or significant change in value.
- Slow down the reporting interval and combine that report by exception feature to achieve higher reporting throughput.

Remote 2008

CONFERENCE AND EXPO

SCADA, Device Networking, M2M, Wireless Technology, Onsite Power, And Security for Remote Sites and Equipment

2008 Call for Papers!

No other industry conference brings together technology users that manage remote sites like the Remote 2008 Conference and Expo. Over 50 conference sessions will provide cutting-edge technology direction and application strategies from the companies and users driving the growth in SCADA, M2M, device networking, data communications, system & site security, emerging wireless technology, remote monitoring and automated control, and onsite powering of distributed equipment, networks and facilities.

Subjects Areas Include:

<ul style="list-style-type: none"> Emerging SCADA Technology Mesh Networking Designing and Implementing New Networks Adapting and Upgrading Existing Networks Device and System Capabilities & Testing Selecting the Right System for Your Application Network Reliability and Accountability Basic Networking Configuration Network configuration in a static environment Basic RF troubleshooting Standards (ISA100, 1451, NERC) Basic network design including IP configurations 	<ul style="list-style-type: none"> Back-up and Stand-by Power Solutions Gen-sets, Fuel Cell and Other Onsite Power Solutions Renewable Energy as a Remote Power Source Power Reliability for 24/7 operation Dual Redundancy of Power for Critical Operations Low Power Systems for Monitoring and Communications Power Protection Systems Substation Automation ROI on Monitoring Technologies Integrating Wireless Technology into existing systems New Wireless Technology for Remote Sites and Equipment Security (Cyber and Physical)
---	---

For more information about submitting a proposal contact Nick Depperschmidt at:
Nickd@infowebcom.com or 800-803-9488 x.111

For more information about sponsoring or exhibiting contact Scott Nash at:
ScottN@infowebcom.com or 800-803-9488 x.114