Wireless Sensor Networks: Implementing Reliable, Simple and Secure Industrial Wireless Solutions

Toteda, S.
Dust Networks, Inc.
30695 Huntwood Avenue
Hayward, CA 94544
USA

Wireless Sensor Networks (WSNs):
Implementing Reliable, Simple and Secure
Industrial Wireless Solutions

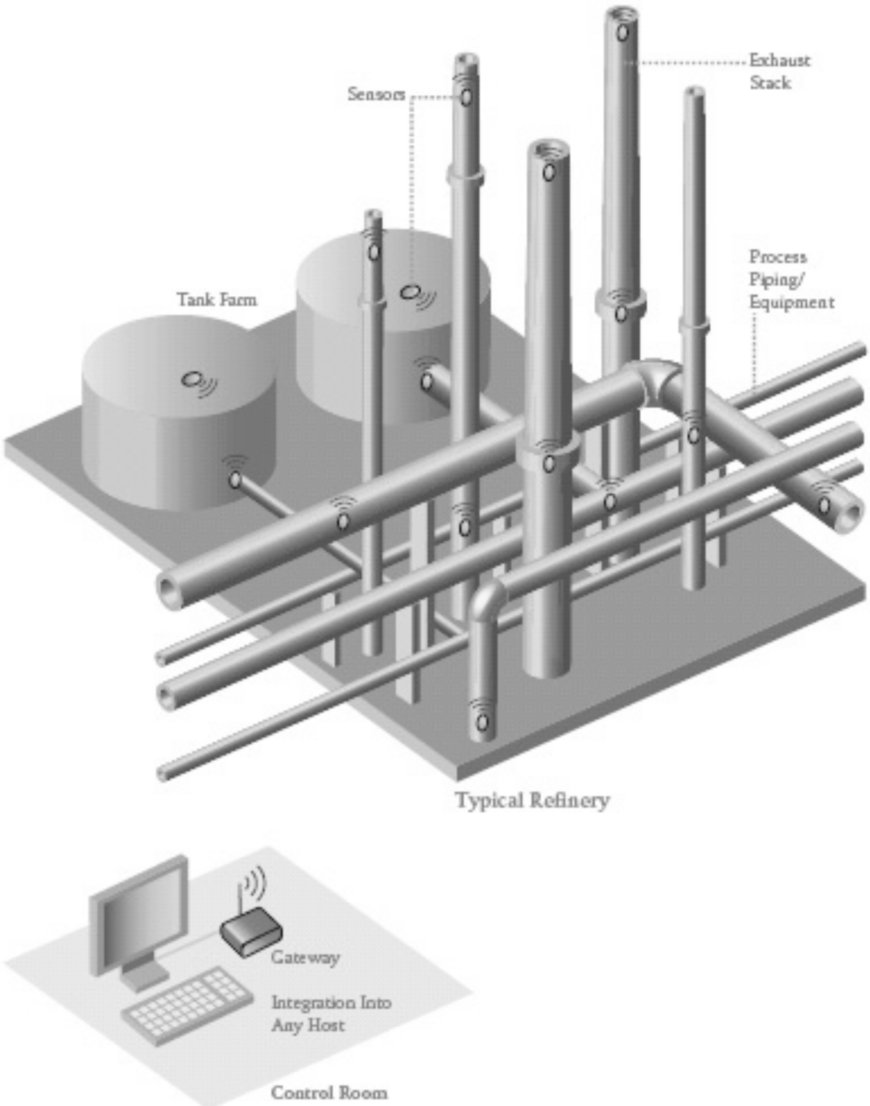

Figure 1. Typical Refinery

The Promise of Wireless Sensing

Wireless sensor networking (WSN) has emerged as a major new technology for the industrial market. With the first wave of industry-standard products now available, we are starting to see the full impact of this technology as users move beyond early pilots and begin to deploy wireless sensors in their production facilities.

The promise of wireless to dramatically reduce the deployment cost of sensors in a production facility primarily comes from eliminating cabling and simplified planning. The cost of cabling can wary widely, and ranges from Euro 100/m to Euro 1,000/m, depending on the safety regulations of the plant. Doing away with the wired network signaling and power cables dramatically reduces the planning and administrative overhead of installing a device. But equally as important is the potential for wireless to make it very easy to deploy sensors in places that simply could not be wired before.

The Importance of Standards

The business imperative is to choose a wireless sensor solution that is based on an industry-accepted standard. While many vendors tout performance, it takes a coalition of vendors to ensure interoperability can be achieved across the industry. This also ensures that future enhancements will be supported through backward compatibility.

Foremost among these standards bodies are HART Communication Foundation with their WirelessHART standard (included as part of HART 7). After years of development, the September 2007 emergence of the WirelessHART protocol opened the door to broad implementation of wireless sensing throughout the industry. Since first made public, many vendors have begun to implement this new capability into their products and process solutions.

Mesh Networks Work

In a typical refinery (Figure 1), the harsh environments created by the complex piping of the production facilities pose serious challenges to wireless sensor technology. These environments are often quite hostile to RF signals; the use of concrete, glass and steel in typical plants exacerbates the traditional RF issues of path loss, fading and multipath.

Successful wireless sensor solutions for monitoring and control systems used in harsh industrial environments require a highly reliable full mesh technology that is field-proven to deliver the performance required. In a mesh architecture, the network can isolate individual points of failure and eliminate or mitigate their impact, allowing the network as a whole to maintain wire-like reliability in spite of local failures.

The wireless mesh network itself is comprised of a group of wireless sensors (called nodes) and a gateway. The nodes are installed at process-critical locations (measuring variables like temperature and pressure) throughout a plant. At regular intervals these nodes “chirp”, broadcasting a packet of collected data. This data is received by a nearby node which in turn forwards the data to the next node. Data is thus transmitted from node to node until it reaches the gateway. At the gateway the information is consolidated and passed through to the controls systems.

In a mesh network, nodes are installed in fairly close proximity to each other (typically less than 100m apart). They, in essence, blanket an area. Each node has the intelligence to seek out and establish communication with other nodes in its network. It can then pass packets of information gathered by its own sensor or by devices that are nearby.

Of course, the purpose of the network is to gather and communicate critical data in a timely, uncorrupted and cost effective manner. To accomplish this, a wireless mesh network must have multiple layers of redundancy as well as low power consumption. Today, the best mesh networks provide three layers of redundancy - path diversity, self-configuration and frequency hopping, as well ultra low power consumption, running for years on a set of standard batteries.

Path diversity allows nodes to work their way around obstructions. A node is both a “parent” and a “child” or, in radio terms, a receiver and a transmitter, and in a mesh network, every node has two parents. Having multiple parents provides path diversity. When a particular path is obstructed, a node can immediately respond to and navigate around it using an alternate path. This multi-path configuration ensures that every node always has at least one back-up (failover) communication path.

Intelligent self-configuration enables nodes to automatically adjust to a dynamic RF environment such as blocked signals and interference. They are self organizing and self healing – when transmission is hindered by something, the network rearranges itself and automatically finds a new path.

Self-configuration also supports a highly scalable network. A new node, with the correct network ID, can be added to the network simply by turning it on. And the network ID, which is included in all communications, allows multiple networks to operate in the same radio space without the risk of sharing data or misrouting information.

Over time, this self-configuring ability drives overall and continuous optimization of the network. The network intelligently seeks the shortest, highest quality transmission paths, re-configuring as circumstances warrant.

In addition to multiple path options, nodes also have channel-hopping options to facilitate working around intermittent RF interferences. Each child to parent connection is called a path. Depending on the radio standard used, each path has a number of channels. For example, using the radio standard IEEE 802.15.4, each path has 16 channels available to communicate on (think 16 radio stations on your radio dial). This frequency diversity enables transmissions to "hop" across all available channels and thus navigate RF interference.

Packets are resent until they are successfully transmitted. The algorithm that sends packets from the child to the parent, trying on a different channel if it does not get through, or trying to send to a different parent if it still does not get through, significantly improves the overall reliability of the system.

We have examined the importance of path diversity, self-configuration and channel hopping to ensure that critical information gets through. One last obstacle to developing a robust, easy-to-use, reliable and truly wireless network is power consumption.

Data transmission consumes power. If a node is continuously transmitting it is it is consuming maximum power and requires either frequent battery replacement or a wired connection to a power source (not a truly wireless network in the latter case).

New standards-based sensors compliant to WirelessHART use time synchronization to reduce power consumption to an absolute minimum. In these systems, all of the nodes share a common sense of time. They transmit, listen or sleep at specified times called timeslots. Timeslots are measured in milliseconds, and in typical applications this leads to a duty cycle of less than 1 percent for all nodes in the network, including those relaying messages for neighboring nodes. Thus these systems are ultra-low-power networking solutions, extending typical battery lifespan to 5 years and more.

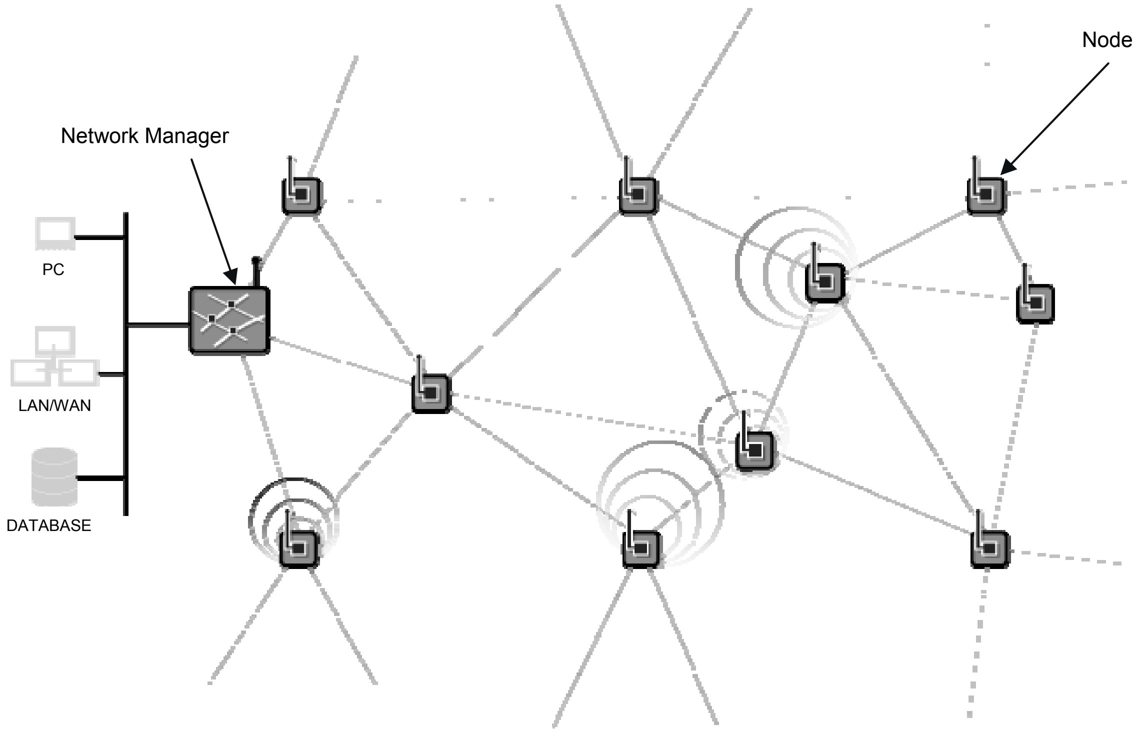

Figure 2. Nodes are pair-wise synchronized with respect to time and frequency for power efficiency and RF-interference avoidance. The manager is continually optimizing data paths to compensate for obstacles and distribute power usage.

Predicting Performance
Wireless sensors operating in challenging environments face RF propagation issues that result in low signal strength and interference. These issues are notoriously difficult to predict during the initial design and provisioning of a WSN. Multipath effects in particular pose problems, and the impact created by the movement of machinery and people is the most difficult to simulate with today's predictive models. Real-world data from industrial environments demonstrates how significant this impact can be and how important it is to accommodate the time-varying effects to ensure reliable network functionality in the face of adversity.

Often a site survey is used to try to predict performance, but the real-time data for an RF link shows markedly different performance at different times of the day.[i] Studies using received signal strength show that the variations are most likely caused by physical changes in the environment around these links, due to equipment and people moving around the factory. The truly dynamic nature of the RF environment in industrial settings requires that the *mesh network itself* perform the equivalent of a site survey in real time and use this data to make the adjustments needed for each transmission.

Conclusion
Proven through rigorous trials, the time synchronized wireless mesh networking technology that underlies the WirelessHART standard has delivered on the promise for wireless to be cost effective to deploy and easy to manage

[i] "*Channel-SpecificWireless Sensor Network Path Analysis",* ICCCN 2007, Lance Doherty (Dust Networks, USA)