Wireless Sensor Networks for SCADA and Industrial Control Systems

Action Nechibvute, Courage Mudzingwa
Department of Applied Physics and Telecommunications, Midlands State University, Private Bag 9055 Gweru, Zimbabwe

ABSTRACT

In traditional supervisory control and data acquisition (SCADA) systems, most sensors are wired, which limits their use. Integrating Wireless sensor networks (WSNs) with SCADA and industrial control systems would make monitoring more flexible. Integrated SCADA and WSN capabilities raise the possibility of realising flexible, maintenance-free systems suitable for most industrial and field operations using low power, battery-operated solutions that offer a low cost, wireless alternative to traditional cabled systems. In this work, we discuss the potential benefits and challenges that are encountered when WSNs are integrated into process automation systems.

Keywords: wireless sensor, networks, SCADA, industrial control, automation

1. INTRODUCTION

The application of Wireless Sensor Networks (WSNs) in industry is gradually being adopted particularly for process monitoring, control and data processing [1-5]. WSN technology brings several advantages over traditional wired industrial monitoring and control systems, including self-organization, rapid deployment, flexibility, and inherent intelligent processing [4]. WSN based automation systems will greatly offer new and more effective functions and solutions which traditionally could not be met through the conventional wired instrumentation systems [3-8].

WSNs are formed from a collection of miniature autonomous devices with sensors embedded in them, called sensor node [6,7]. A typical node include the following basic components: power unit, sensor unit, processing unit, memory unit and communication unit (See Figure 1). The power unit is usually a battery, which acts as the power source for all the components of the sensor nodes. It is important that the sensor network should be able to perform the monitoring operations of the environment for a sufficient time (which could be days or months). The battery lifetime may not be compatible with the expected performances of the node; it is therefore required to scavenge energy from the external environment [8-10]. The sensor unit consists of a group of micro-electromechanical system (MEMS) - based sensors (and actuators) used for data acquisition from the physical environment. The processing unit which includes a microprocessor or a micro-controller is responsible for management of data acquisition, handling communication protocols, scheduling and preparation of data packets for transmission once it has gathered, filtered, and synchronised the data from the sensors [10-13]. The communication unit consists of a short range RF transceiver for wireless communication. The individual nodes are capable of sensing their environments, processing the information locally, or sending it to one or more collection points through a wireless link [11,12]. WSNs present a novel technology, which has advantages of distributed information processing, broad coverage, and remote monitoring and control [6,7,12].
improving the sensing capabilities of SCADA sub-systems, as well as of increasing the resilience of the overall SCADA architecture.

In this paper we discuss the adoption of WSNs as an integral part of the next generation SCADA and industrial control systems. The paper is organized as follows: Section 2 provides an overview of SCADA and SCADA systems. Section 3 discusses the industrial WSNs, Section 4 overviews the industrial WSNs for SCADA and process automation. Section 5 discusses the challenges and potential solutions that need to be addressed for successful integration and applicability of wireless instrumentation. Finally, the paper is concluded in Section 6.

2. OVERVIEW OF SCADA SYSTEMS

2.1 Components of SCADA Systems

SCADA is a technology that enables the user to collect data from one or more distant facilities and/or send limited control instructions to those facilities [13]. It can be alternatively described as a system operating with coded signals over communication channels so as to provide control of RTU (Remote Terminal Unit) equipment [13-15]. Traditionally, the majority of SCADA systems are designed for more closed and controlled industrial environments. However, there has been an integration of enterprise systems and large scale services to enhance their functionality while minimizing overall operation cost.

A typical SCADA System consists of several subsystems notably [14-17]:

1. Field data interface devices: Remote Terminal Units (RTUs) or Programmable Logic Controllers (PLCs) which collect data from the field deployed sensors make the necessary adjustments and transmit the data to the monitoring and control system. PLCs are frequently used as alternatives to RTUs since they are more economical, versatile, flexible, and configurable than special-purpose RTUs [18].

2. The communication infrastructure used to transfer data between field data interface devices and control units and the computers in the SCADA central host. The infrastructure can be radio, telephones, cables, satellites, or any combination of these.

3. A central host computer server or servers (sometimes called a SCADA Centre, Master Station, or Master Terminal Unit (MTU). The computer does the monitoring (gathering of data) as well as the control (actuation) of the linked processes.

4. A collection of standard and/or custom software sometimes called Human Machine Interface (HMI) software or Man Machine Interface (MMI) software systems used to provide the SCADA central host and operator terminal application, support the communications system, and monitor and control remotely located field data interface devices.

When SCADA systems were first developed, the concept of computing in general centred on “mainframe” systems [17]. Networks were generally non-existent and each centralized system stood alone. As a result, first generation SCADA systems were standalone and monolithic with virtually no connectivity to other systems. The Wide Area Networks (WANs) that were implemented to communicate with remote terminal units (RTUs) were designed with a single purpose in mind: –that of communicating with RTUs in the field and nothing else. However, the next generation of SCADA systems took advantage of developments and improvements in system miniaturization and Local Area Networking (LAN) technology to move towards a more distributed flavour where LAN was used to interconnect the components (see Figure 2). This approach was more cost effective than the first generation and allowed distributed processing and real-time information sharing among the entities based on proprietary protocols [17,18]. As was the case with the first generation systems, the second generation SCADA systems were also limited to hardware, software, and peripheral devices that were provided or at least selected by the vendor. The emergence of the third generation moved towards utilizing the network as such, using not only WAN but also Internet, and featured open system architecture and open protocols [15,18]. The distributed processing across physically separate locations has enabled the design of SCADA systems that can survive a total loss of any one location. For some organizations that see SCADA as a super-critical function, this is a real benefit. The next generation will push further the limits in the network, adopting WSNs to enhance the capabilities of SCADA systems [5,18].

2.2 Challenges to conventional SCADAs

While SCADAs are the mainstay of most automation systems in industry, they have their own challenges. As noted by Ye [20],
the major challenge of conventional SCADA systems is their inflexibility, static and centralized architecture which significantly limits their interoperability with other networks technology or systems. Generally SCADA systems are expensive to deploy and maintain. This is particularly so for applications such as pipeline network in oil and gas fields [19]. Proprietary SCADA systems tie their customers to one specific control device manufacturer, creating a difficult negotiating position for customers during future purchases [20]. Legacy SCADA systems which still dominate the automation and telemetry implementations lack compatibility with other systems and thus limit scalability. SCADA has low data and low data update rates making it inefficient in such systems as Smart Grid Applications [21-23].

2.3 Potential benefits of WSNs in SCADA and Automation

Reduced Maintenance and Deployment Costs: Wireless sensor nodes eliminate cabling and trenching cost of deployment by up to 70% [24]. Unlike its wired counterpart, wireless devices can be deployed in areas that are both physically inaccessible and cost prohibitive for example - monitoring and control devices for rotary equipment [25]. WSNs offer easy maintenance since problems like corrosion, water in the conduit, burned cabling, freezing, wild animal damage, , and physical wear caused by frequent encounter in wired systems are eliminated.

High levels of Scalability and Flexibility: Wireless devices can be easily relocated and reorganized without tedious work of removing old cables and laying out new ones [24,25]. Furthermore, the industrial process system becomes highly scalable and flexible due to the device autonomy [25-28]. Wireless systems are battery powered, newly added devices can be installed at any location without running power supply and data communication wires through concrete walls during factory expansion. On the contrary, wired systems can take days or weeks to install, whereas wireless instruments require only the sensor to be installed in the process, saving time and valuable resources. The rigid design of current RTUs reduces the flexibility of SCADA systems [19,20].

Improved Resource management in a control system: WSN enabled systems make real-time decisions based on measurements taken while an industrial process is running. Measurement data from the wireless sensors can be readily utilized for both dynamic control of industrial process and display over a network to allow remote monitoring of the process status in real-time. Abnormal conditions (e.g. rising or falling pressures, temperatures, or vibrations) may be easily flagged up as fault conditions. As data is collected as part of a SCADA system, it can also be archived for future reference [29-31].

Improved Performance: WSN enabled automation systems have the potential to outperform the existing wired process control systems. Firstly, industrial WSNs allow higher data transmission speed. For example, the most popular control protocols HART (Highway Addressable Remote Transducer) has a data rate of 1.2 kbps and FF (Foundation Fieldbus) has a data rate of 31.25 kbps, while WirelessHart has a data rate of 250 kbps based on the IEEE 802.15.4 standard. Secondly, unlike wired control systems, where devices share a single bus, multiple wireless communications can act simultaneously if there is no mutual radio interference [25,30]. Thirdly, more sensors/data points can be used to beat the performance of traditional wired control system.

Exploitation of Micro-Electromechanical Systems (MEMS): MEMS devices integrated with computational power and communication capabilities offer a more robust design than attaching wires to small-sized devices [32]. This means embedded sensor systems can be applied widely, including in production lines, (See Figure 3).

![Figure 3 Application of WSNs in production line](image)

Table 1: comparison between SCADA and WSN[19]

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>SCADA</th>
<th>WSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecture</td>
<td>Centralized</td>
<td>Decentralized</td>
</tr>
<tr>
<td>Storage &amp; Control</td>
<td>Central site</td>
<td>Local Sensor node</td>
</tr>
<tr>
<td>Flexibility</td>
<td>Inflexible</td>
<td>Versatile</td>
</tr>
<tr>
<td>Cost</td>
<td>Expensive</td>
<td>Low</td>
</tr>
<tr>
<td>Node Density</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Data Rate</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Network Protocol</td>
<td>Proprietary</td>
<td>Non-proprietary</td>
</tr>
</tbody>
</table>

3. INDUSTRIAL WSN REQUIREMENTS

3.1 Application Specific Requirements

There are strict regulations that govern the installation of wires in some industrial environments, particularly in the oil and gas sector. As a result of the strict regulations associated with the installation of wired sensors on oil and gas platforms, the introduction of WSN devices is complicated, time-consuming
and expensive. WSNs deployments in such environments and manufacturing industries need to be highly reliable and compatible with the existing wired systems. The performance of these sensors often determines the success of the manufacturing operation itself. If the sensors do not perform their mission large amounts of valuable production or production time may be lost. Wireless sensors need to be designed specifically to fulfill an industrial mission in the presence of many types of radio interference. The sensor network must be able to perform its operation in a distributed manner. These sensors often determines the success of the manufacturing process automation. The ISA SP100 workgroup classified the industrial processes into three broad categories and six classes of WSN usage (from Class 0 to Class 5) as shown in Table 2 [34]. Table 3 shows some of the network requirements in industrial process automation.

The design of networked control systems has to take into account a large number of factors that ensure correct implementation and different industrial applications will have very different needs and will choose different solutions, values, or bounds for each of these variables. The real objectives for any wireless industrial product are determined by the manufacturing operation in which it must perform, not by the technology employed. Some of the most critical requirements are system performance in terms of data transmission rate and sample rate, communication reliability and power supply. The last one is especially critical in the context of WSNs, because the network must be able to operate for long periods without the need of battery replacement. Reliability is required. Wireless instrumentation must be as reliable as conventional wired units. Radio interference is always a concern, and the sensor network must be able to perform its service, which would require human involvement. In addition to automatic network initialization, self-diagnostic and self-healing operations, it is also important to be able to perform intelligent operations in the network in a distributed manner.

### Table 2: Application needs of industrial process by usage [34]

<table>
<thead>
<tr>
<th>Safety</th>
<th>Class 0: Emergency action (always critical)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>Class 1: Closed loop regulatory control (often critical)</td>
</tr>
<tr>
<td></td>
<td>Class 2: Closed loop supervisory control (usually non-critical)</td>
</tr>
<tr>
<td></td>
<td>Class 3: Open loop control (human in the loop)</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Class 4: Alerting; Short-term operational consequence (e.g event based maintenance)</td>
</tr>
<tr>
<td></td>
<td>Class 5: Logging &amp; downloading/uploading No immediate operational consequence (e.g history collection, preventative maintenance)</td>
</tr>
</tbody>
</table>

### Table 3: Typical requirements for industrial wireless sensor and actuator networks in the process automation domain [35]

<table>
<thead>
<tr>
<th>Sensor Network Applications</th>
<th>Delay</th>
<th>Range</th>
<th>Battery Lifetime</th>
<th>Update Frequency</th>
<th>Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring and supervision</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vibration sensor</td>
<td>S</td>
<td>100 m</td>
<td>3 years</td>
<td>Sec-days</td>
<td>Low</td>
</tr>
<tr>
<td>Pressure sensor</td>
<td>Ms</td>
<td>100 m</td>
<td>3 years</td>
<td>1 sec</td>
<td>Low</td>
</tr>
<tr>
<td>Temperature sensor</td>
<td>s</td>
<td>100 m</td>
<td>3 years</td>
<td>5 sec</td>
<td>Low</td>
</tr>
<tr>
<td>Gas detection sensor</td>
<td>ms</td>
<td>100 m</td>
<td>3 years</td>
<td>1 sec</td>
<td>Low</td>
</tr>
<tr>
<td>Closed loop control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control valve</td>
<td>ms</td>
<td>100 m</td>
<td>5 years</td>
<td>10-500ms</td>
<td>Medium</td>
</tr>
<tr>
<td>Pressure sensor</td>
<td>ms</td>
<td>100 m</td>
<td>5 years</td>
<td>10-500ms</td>
<td>Medium</td>
</tr>
<tr>
<td>Temperature sensor</td>
<td>ms</td>
<td>100 m</td>
<td>5 years</td>
<td>500ms</td>
<td>Medium</td>
</tr>
<tr>
<td>Flow sensor</td>
<td>ms</td>
<td>100 m</td>
<td>5 years</td>
<td>10-500ms</td>
<td>Medium</td>
</tr>
<tr>
<td>Torque sensor</td>
<td>ms</td>
<td>100 m</td>
<td>5 years</td>
<td>10-500ms</td>
<td>Medium</td>
</tr>
<tr>
<td>Variable speed drive</td>
<td>ms</td>
<td>100 m</td>
<td>5 years</td>
<td>10-500ms</td>
<td>Medium</td>
</tr>
<tr>
<td>Interlocking and Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proximity sensor</td>
<td>ms</td>
<td>100 m</td>
<td>5 years</td>
<td>10-250ms</td>
<td>Medium</td>
</tr>
<tr>
<td>Motor</td>
<td>ms</td>
<td>100 m</td>
<td>5 years</td>
<td>10-250ms</td>
<td>Medium</td>
</tr>
<tr>
<td>Valve</td>
<td>ms</td>
<td>100 m</td>
<td>5 years</td>
<td>10-250ms</td>
<td>Medium</td>
</tr>
<tr>
<td>Protection relays</td>
<td>ms</td>
<td>100 m</td>
<td>5 years</td>
<td>10-250ms</td>
<td>Medium</td>
</tr>
</tbody>
</table>

### 3.2 Performance Issues

In this section we discuss some major issues that need to be addressed in order to achieve a large scale deployment of WSNs in industrial automation.

**Reliability:** It is the measure of the percentage of accurate data which reaches its destination. The ability of the network to ensure reliable data transmission in a state of continuous change of network structure [35-37]. Packet loss in wireless sensor networks is usually due to the quality of the wireless channel, sensor failure, and congestion. Most of the applications need reliable transmission of each packet, and thus packet-level reliability is required. Wireless instrumentation must be as reliable as conventional wired units. Radio interference is certain, and the sensor network must be able to perform its mission in the presence of many types of radio interference.

**Scalability:** It is the ability of the network to grow, in terms of the number of nodes, without excessive overhead—represents...
the maximum number of generated key rings which corresponds to the maximum number of supported nodes [38]. A large scale secure deployment of sensor networks relies strongly on this performance metric [38-41]. The number of sensors in a single production unit can vary from a few to several thousands.

**Adaptability:** It is a measure of time delay. It is defined as the time it takes from when a data packet is transmitted from the originating sensor to reach its final destination [42].

**Latency:** The time required for a sensor reading to reach the automation system must be bounded if the sensor data is used in a closed-loop control system. The upper limit of this bound depends upon the application. It can range from seconds to just a few milliseconds [43,44]

**Control loop cycle times:** Process automation control loop cycle times are normally in the range of seconds to minutes, while machine control loop cycle times are normally in the range of milliseconds [45,46].

**Range:** The sensor network will need to communicate reliably over a specified distance. Some production equipment is compact, and some is very large. Multiple wireless hopping is typically employed since the inter-sensor communication is within short transmission ranges due to energy and bandwidth limitations [47].

**Power Efficiency:** This is the ability of the network to operate at extremely low power levels. The sensor will need reliable battery power (with its disadvantage of additional service intervals) or some other source of energy. The lack of battery replacement, which is essential for affordable WSN deployment, requires energy-efficient operations. Since high reliability and low delay may require significant energy consumption, the reliability and delay must be flexible design parameters that still meet the requirements [48,49].

**Data Types:** There are both analog and discrete output sensors, and in addition some “smart” sensors may supply diagnostic information that can also be used to improve the reliability or quality of production.

**Sensor Traffic Patterns:** The type and amount of data to be transmitted is also important when considering control applications [47-49]. Control signals can be divided into two categories: real-time and event based. For real-time control, signals must be received within a specified deadline for correct operation of the system. In order to support real-time control, networks must be able to guarantee the delay of a signal within a specified time deadline. Hence, heavy traffic may be generated if sensors send data very frequently. Event-based control signals are used by the controller to make decisions but do not have a time deadline [50]. The decision is taken if the system receives a signal or a timeout is reached.

4. **INDUSTRIAL WSNs FOR SCADA & PROCESS AUTOMATION**

4.1 WSN Interfacing Automation Systems

WSNs are principally an enabling technology that can further push the limits of the current networked SCADA systems. Firstly, the WSNs can be potentially used as a replacement for the remote terminal units (RTUs) in conventional SCADA systems. In the context of wireless automation, WSN usually operates as a part of the automation system and hence issues of interfacing and compatibility with other parts of the system are critical. It must be noted that the WSNs for SCADA systems are unique; and are different from the generic WSNs. The key differences to be noted are [51]:

- There is an online trusted third party (monitoring station).
- There is no aggregation: the controller collects all the data coming in from the sensors.
- The battery life of the sensors is expected to last several years; therefore, the energy efficiency of the protocols is not as critical as in other applications of sensor networks.
- Although there are some implementations of multi-hop routing, the majority of current deployments use a single hop between the sensors and the gateway.
- Sensors must be accessible and configurable by handheld devices used by network operators.

WSNs can be interfaced to SCADA systems and other wired automation control platforms by means of specially designed middleware. The middleware frameworks can be used to capture the data from the WSNs and distribute pre-sorted and translated information to the SCADA system. A practical example is SensiLink™ which is a middleware and software suite from MeshNetics that links WSNs with SCADA systems [52,54]. Sensor data collected from the nodes is channeled through RS232, RS485, USB, Ethernet, or GPRS gateway to the SensiLink server. ArchRock [55], OctaveX [56], and SnapSense OneClick [57] are some of the middleware that can be used in the integration of WSNs to the process automation platforms. Alternative approaches can also be realised by means of Peer to peer (P2P) protocols (for example HourGlass [58] and P2PBridge[59,60]) and the use of sensor network gateways functioning as bridges [61,62]

4.2. Industrial WSNs for Process Automation

ZigBee [63], WirelessHART [64] and ISA100.11a [65] are the most popular standards for industrial wireless devices and networks [66]. Unlike the ZigBee standards which are insufficient to fulfil the strong reliability requirements of
process automation, the WirelessHART and ISA100.11a standards offer the most complete set of mechanisms with channel blacklisting and frequency hopping to avoid perturbations caused by interference. Major international automation and control companies have developed applications of wireless instrumentation technologies based on the WirelessHART and/or ISA100.11a. The companies of note in this field are Honeywell [67], Emerson [68], ABB [69], Rockwell [70] and Yokogawa[71]. This section discusses the fundamentals of WirelessHART and ISA100.11a networks.

(a) WirelessHART network: System overview

The following devices and components are associated with a WirelessHART network [64]:
1. Field Device: A field instrument with integrated wireless communication.
2. Adapter: A wireless communication module that connects to wired HART field devices, providing them with WirelessHART capabilities.
3. Handheld: A portable WirelessHART computer used for configuration, diagnostics, and calibration of field devices.
4. Gateway: A network access point that connects the WirelessHART network to a plant automation network, allowing the data to flow between the two.
6. Security Manager: An application that is responsible for generating, storing, and managing join, network, and session keys.

(b) ISA 100.11a: System overview

An ISA100.11a device shall hold one or more of the following roles [65]
1. Input/Output (I/O): A device that provides data (sensor) to or uses data (actuator) from other devices.
2. Router: A device that is capable of routing data from other devices in the network.
3. Provisioning: A device that is capable of provisioning other devices, enabling them to join a specific network.
4. Backbone Router: A device that is capable of routing data to/from a backbone network.

5. Gateway: A device that provides an interface between the wireless and the plant network or directly to an end application on a plant network.
6. System Manager: An application that governs the network, network devices, and network communications.
7. Security Manager: An application that, in conjunction with the system manager, provides a secure system operation.
8. System Time Source: A device that is responsible for maintaining the master time source for the system.

Figure 4 Network Elements: WirelessHART and ISA100.11a [64,65]

The reader is referred to [72] for details of the competing features of WirelessHART and ISA100.11a standards. Table 4 gives a review of the standards.

Table 4: Table 5 ZigBee, WirelessHART, and ISA100 Characteristics [38,63-65,72]

<table>
<thead>
<tr>
<th>Protocol layers</th>
<th>ZigBee</th>
<th>WirelessHART</th>
<th>ISA100.11a</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHY layer</td>
<td>IEEE 802.15.4-2003 with 868 MHz/915 MHz or 2.4 MHz radio</td>
<td>IEEE 802.15.4-2006 with 2.4 MHz radio only</td>
<td>IEEE 802.15.4-2006 with 2.4 MHz radio only</td>
</tr>
<tr>
<td>MAC layer</td>
<td>IEEE 802.15.4-2003 with a low frequency hopping schema. No deterministic access methods</td>
<td>IEEE 802.15.4-2006 with TDMA + Channel hopping or Token-passing method</td>
<td>IEEE 802.15.4-2006 with an extension shim for frequency hopping and slotted hoping No deterministic access methods</td>
</tr>
</tbody>
</table>
### Network Topology

<table>
<thead>
<tr>
<th></th>
<th>Star, Mesh</th>
<th>Tree, Star, Mesh</th>
<th>Star, Mesh</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Scalability</strong></td>
<td>16-bit node address and 16-bit group address or 64-bit extended network address</td>
<td>16-bit network address, 16-bit nickname and 64-bit address</td>
<td>64-network address and 64-bit device address</td>
</tr>
<tr>
<td><strong>Network routing Strategy</strong></td>
<td>Mixed mechanism composed of AODV and tree routing No energy aware routing strategy</td>
<td>Graph routing (link state routing) No energy aware routing strategy</td>
<td>Graph routing (link state routing) No energy aware routing strategy</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>A mesh-networking standard for control and monitoring; building/home automation, embedded sensing. Range of up to 50m</td>
<td>A multi-vendor standard specifically designed for process monitoring and control; mesh networking with large numbers of sensors/nodes. Range is less than 100 feet</td>
<td>A multivendor standard for reliable and secure wireless connectivity for Non-critical control and monitoring. Low data rate, very low power consumption. Range of 600m</td>
</tr>
<tr>
<td><strong>Advantages</strong></td>
<td>Low-cost, power efficient, easy solution for small networks. Use is wide spread</td>
<td>Designated as an international standard. Built on a 30-year old HART technology. An accepted standard. Specifically created for industrial controls</td>
<td>Can scale above 250 nodes per network. An accepted standard. Created specifically for industrial controls</td>
</tr>
<tr>
<td><strong>Disadvantages</strong></td>
<td>Cannot serve a high number of nodes within the specified period</td>
<td>Not compatible with some existing wired protocols (FieldBus, Profibus) Up to 250 nodes on a network</td>
<td>Not yet in wide use. Communicates with HART, Fieldbus Modbus, Profibus</td>
</tr>
</tbody>
</table>

---

5. CHALLENGES AND POTENTIAL SOLUTIONS

1) **Harsh Industrial conditions**

The harsh industrial conditions present a challenging operating environment for WSNs and the associated wireless device. The WSN are expected to work reliably over a range of operating temperatures, and to sustain strong vibrations, excessive electromagnetic noise caused by large electromechanical equipment [73]. In addition to this noisy environment, the WSNs should withstand the atmospheric precipitation, condensation and airborne contaminants present [74, 75]. Furthermore, the signal might be subject to heavy multipath propagation effects caused by multiple reflections from mainly metallic structures in the surrounding environment. The random/periodic movement of workers, industrial robots, trucks, and other objects may also cause time varying channel conditions. These propagation impairments to mission-critical signals in industrial settings can result in costly disasters in terms of money, manpower, time, and even human lives [76, 77]. The Direct Sequence Spread Spectrum (DSSS) or Frequency Hopping Spread Spectrum (FHSS) technology has been utilized to significantly reduce noise interference. Redundant technique—dual gateways are highly recommended for increased reliability [25]. However, more research efforts on designing the WSN for industrial environments is needed. A typical research approach is investing in WSN testbeds (for example WINTeR [78]) that mimic the industrial surroundings with complex multipath propagation schemes. Better still would be intensive study using testbeds such as GINSENG [79].
2) Data and Network Security

Sensor nodes are not tamper resistant due to cost constraints; any human user or machine can reprogram them or simply destroy them. Passive attacks on WSNs are able to retrieve data from the network, but do not influence over its behaviour. On the other hand, active attacks directly hinder the provisioning of services [80]. These security attacks directly affect the energy consumption and due to the large amount of energy consumed at the MAC layer, it is particularly vulnerable to many different security attacks. More research on behavioural modelling of security attacks is needed [81]. Currently, the wired fieldbuses connecting SCADA and automation system to WSN devices lack security extensions. This loophole is potentially a severe challenge since scalable and modular solutions cannot be provided when integrating new wired/wireless devices into existing automation systems [82]. To secure IP-based SCADA systems, it is vital to implement secure architectures which prevent access to the SCADA from corporate IT and other third-party networks and to enforce excellent management practices to manage IP-based networks [83]. As noted by Cardenas et al [84], there are many research challenges that need to be addressed particularly the development of systematic analysis of the threat model and its relation to the security countermeasures, the precise definitions of security metrics, and the detailed study of real world deployment scenarios.

3) Quality of Service (QoS) Issues and resource constraints

The deployment strategies of WSN in industrial automation systems for coverage and connectivity enhancement are critical to the (QoS) of the networks. The guarantee of QoS typically considers multiple factors, for example, electromagnetic interferences, accidental death of sensor node, dynamic network topology, low processing capability, and small memory capacity [85]. Furthermore, the design and implementation of WSNs is constrained by three types of resources: a) energy; b) memory; and c) processing [7,11,51];- which makes it hard to maintain the QoS [86]. Current research output on energy harvesting and novel energy management will potentially contribute significantly in addressing the energy constraints in WSNs. However, due to refresh rates required in process automation it is difficult to save much energy by minimizing the duty cycle of a wireless field device [87].

6. CONCLUSIONS

In this article, a discussion of the main issues involved in the application of WSNs in SCADA and industrial control systems. There is need for efficient integration of the WSNs into existing automation to achieve a seamless transition from wired to wireless communication, as well as simple deployment, commissioning, and maintenance. Despite outstanding research issues on security, reliability and QoS, WSN-enable automation systems will get more popular, largely due to the greatly increased flexibility, lower cost and scalability that could not be obtained from the traditional all-wired automation systems.

REFERENCES


[29]. Wireless sensors enjoy timely role in factory automation: Industrial Ethernet Book Issue 57 / 35; http://www.iebmedia.com


