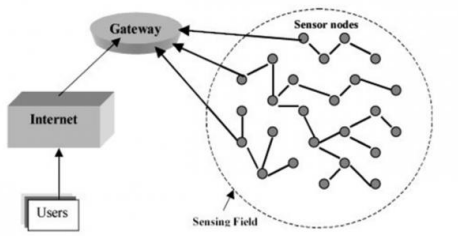
Evolution of industrial wireless sensor networks: Page 4 of 5

November 10, 2017 // By Mark Miller, L-com Global Connectivity, Wireless Product Manager



Industrial automation powered by wireless sensor networks (WSN) is heralding the Industrial Internet of Things and Industry (IoT) 4.0. Key enabling cloud and wireless mesh networking technologies promise to bring multi-year battery life, IP addressability to machines and sensors, cloud-based provisioning and management systems, as well as fieldbus tunneling.

Wired networks such as controller area networks (CAN) for automobiles would have to experience a BER of no more than 10^{-6} in order to have undetected corrupted messages occur less than once per year for the vehicle fleet [8] while the popular MIL-STD-1553B for avionics boosts BERs as low as 10^{-12}. Most IWSN standards leverage a combination of Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), and Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) of medium access control (MAC) protocols. The main difference between wired and wireless MAC protocols generally stems from the ability to detect collisions on the medium while sending (e.g.: CSMA/CD) [9]. Since this is not possible over the wireless medium, quality of service (QoS) analysis can be leveraged in IWSNs to measure packet loss, bandwidth, and delay. Moreover, additional MAC protocols can be utilized to increase the determinism of WSN.

Preliminary models are also being proposed that leverage binary countdown protocols [9], employ a collision-free MAC protocol [10], attempt to approximate carrier sense multiple access with collision detection (CSMA/CD) using the proposed carrier sense multiple access with collision notification (CSMA/CN) [11], uses an additional carrier sensing (ACS) algorithm to enhance the carrier sensing mechanism in the IEEE 802.15.4 CSMA/CA protocol [12], and leverages new channel access mechanism for a low latency deterministic network (LLDN) superframe in a star topology [13]. The CSMA/CA protocols generally suffer energy waste due to collisions and unpredictable end-to-end delays so TDMA mechanisms are employed in standards such as WirelessHART and ISA100.11a for a more assured QoS with reservation-based medium access. Improvements over these standards are proposed that use a time-synchronized mesh network with short time slots where the device and overarching network operations are synchronized [14].

Security

Security ranks amongst the top concerns for IWSN end users (Figure 2). As shown in Table 1, there are several major aspects to security including data confidentiality, integrity, availability, freshness, and authenticity [15]. Strengthening all these aspects of security protect an IWSN against both passive (e.g.: transmission eavesdropping and sniffing) and active attacks (e.g.: physical modification, Denial of Service, data falsification, and interruptions of service).

Dimensions of Security	Description	Example	WSN Protections
Data Confidentiality	Ensures highly sensitive information is encrypted and cannot be leaked.	Sniffing	Access Control List (ACL), Public-Key Cryptographic (PKC), AES-128
Data Integrity	Ensures data is not altered in transit.	Data manipulation	Message Integrity Check (MIC), Public-Key Cryptographic (PKC), AES-128
Data Freshness	Ensures data is recent.	Replay Attack	Time Synchronization Schemes
Data Authenticity	Ensures data is sent from correct source.	Spoofing	Message Authentication Code (MAC), Join Key, Challenge-Response, IEEE 802.1X

Table 1: Dimensions of security.

previous 1 2 3 4 5 next

Design category:
Wireless Communications