

Reliable and Secure Wireless Networks

A few of the important advantages in using wireless networks for collecting data from remote sensors in industrial environments include lower installation and maintenance costs, greater physical mobility and freedom, and faster commissioning of services. However, an important characteristic of industrial environments is the presence of an abundance of metal-based structures scattered in a small geographic area which tend to severely hinder proper wireless transmissions in that area. Typically, waves are reflected off metallic surfaces and waves reach their destination through multiple paths which serve to considerably attenuate wireless signals between the transmitter and the receiver. Chiefly, reflection, diffraction, and scattering occur from metal surfaces in industrial environments; reflections occur from surfaces whose dimensions are larger than the wavelength (which is about 3 cm at 2.4 GHz) such as the earth's and industrial structures and at the receiver the reflected waves may cause interference with the directly received waves. Diffraction occurs when secondary waves are created behind impenetrable metal structures and permits non-line of sight transmission of wireless energy between the transmitter and receiver; scattering occurs from surfaces that are of same or smaller dimension than the transmitted wavelength and causes waves to radiated in different directions. The resulting attenuation caused by metal surfaces can be between 13-19 dB at 2.4GHz and 25-32 dB at 5 GHz, and the signal strength fades about 20 dB faster than free space propagation fading. Due to these effects on wireless transmissions in industrial environments, bit error ratio (BER) of wireless transmissions also tends to be higher than in open space transmissions. Even when Forward Error Correction (FEC) and ARQ (Automatic Repeat Requests) are used frame losses tend to be relatively high while effective throughput is significantly reduced. Bit error ratios of 10^{-4} to 10^{-2} have been observed and packet losses in excess of 10% have been observed in industrial environments. Therefore, reliability of wireless transmissions in industrial environments is lower compared to open space. Moreover, since wireless transmissions can be relatively easily intercepted, security of wireless transmissions is also lower than that provided by wired connections. There are two main security issues for wireless transmissions in industrial environments: since the transmissions are essentially broadcasted unauthorized users can access transmitted signals, and imposters (devices included) could hijack transmission medium to deny services for other legal users. Techniques used to improve security include using spread spectrum radio, proprietary protocols such as Zigbee, and network topology such as mesh configuration that improves security in wireless networks in combination with other techniques.

At CPSR we plan to develop reliable and secure wireless link-layer protocols to help users of SCADA systems significantly reduce their installation and maintenance costs. We developed the RESILIENT protocol for this purpose. Fig. 1 illustrates the architecture of RESILIENT. The data packets containing measurement information such as pressure, temperature are stored at the receiver's buffer. Further, the Packet Distortion Estimator (RDE) component measures the expected distortion in arriving packets. RDE uses received signal strength indication (RSSI) and link quality indication (LQI) as side information in every transmission. All receivers compliant with the IEEE 802.15.4 standard are required to measure RSSI and LQI for each transmission. The objective is to

train the Markovian channel model to achieve accurate estimations of BERs. This information is then provided to the Packet Management (PM) module. This module uses the optimization problem to specify the optimal data and parity bits allocations for the next data transmission at the sender side. In addition, PM performs packet encoding/decoding at the sender/receiver side using Reed-Solomon (RS) codes.

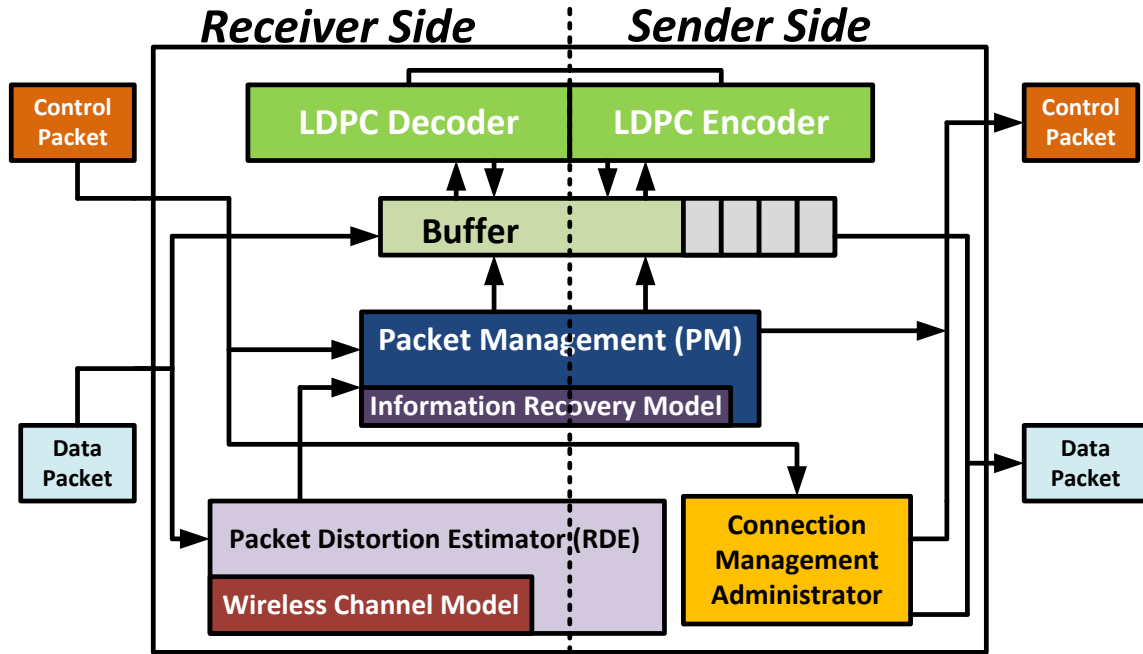


Figure 1. Architecture of RESILIENT Protocol