Deployed Sensor Networks and Their Security Challenges in Practice

Erdal Cayirci
University of Stavanger/NATO Joint Warfare Centre
Stavanger, Norway
erdal.cayirci@uis.no

Abstract

Wireless sensor networks (WSN) have many security and safety applications. Wireless sensor networks for pipeline security, border security and blue force tracking are among the emerging WSN security applications. These are heterogeneous systems where various kinds of sensing, surveillance, networking and command/control (C2) technologies are integrated. They are typically based on the deployment of a large number, i.e., hundreds of thousands, of unattended nodes for extended time periods. The nodes can be in a distance of several hours from physical reach. Some parts need to be deployed and redeployed rapidly, and rely on battery power on board. Therefore, scalability, fault tolerence and power awareness are critical factors influencing their design.

They are also susceptible to security threats different from typical military and commercial systems. One may claim that the biggest risks can be denial of service attacks in physical layer, i.e., jamming, and attacks against integrity and confidentiality. We believe that the most important security challenges are related to denial of service attacks, especially in MAC, network and transport layers, and special attacks developed against the schemes like node localization, time synchronization, and event detection.

In our talk, we first briefly introduce pipeline security, border security and blue force tracking applications, and their available commercial on the shelf products. Then elaborate the security threats and required security mechanisms for them. We also give our solutions for some of these security challenges and results obtained from their practical implementation and deployment cases.