ISBN: 978-93-5780-385-4

Identifying Selective Forwarding Attacks in Wireless Sensor Networks using Multiple Resources

N.Sarita Rani

Assistant Professor, Department of Electronics and Communication Engineering, Dadi Institute of Engineering and Technology, Anakapalli, Jawaharlal Nehru Technological University Kakinada

Abstract: A Wireless Sensor Network (WSN) consists of distributed an autonomous devices that monitors both physical and environmental conditions. Sensor Networks are used for weather prediction and measuring temperature, sound, wave, vibration, pressure etc. Sensor Networks suffer from various security attacks such as sink hole attack, black hole attack, wormhole attack and selective forwarding attacks. Selective forwarding attack happens in compromised nodes by dropping packets selectively. This paper surveys various techniques for detecting selective forwarding attacks in WSNs. A wireless sensor network (WSN) has important applications such as remote environmental monitoring and target tracking. This has been enabled by the availability, particularly in recent years, of sensors that are smaller, cheaper, and intelligent. These sensors are equipped with wireless interfaces with which they can communicate with one another to form a network. The design of a WSN depends significantly on the application, and it must consider factors such as the environment, the application's design objectives, cost, hardware, and system constraints.

Keywords: Wireless Sensor Network, Selective Forwarding Attacks, Compromised Nodes, CHEMAS Technique.

Introduction

Wireless sensor networks (WSNs) have gained worldwide attention in recent years, particularly with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology which has facilitated the development of smart sensors. These sensors are small, with limited processing and computing resources, and they are inexpensive compared to traditional sensors. These sensor nodes can sense, measure, and gather information from the environment and, based on some local decision process, they can transmit the sensed data to the user. Smart sensor nodes are low power devices equipped with one or more sensors, a processor, memory, a power supply, a radio, and an actuator.1 A variety of mechanical, thermal, biological, chemical, optical, and magnetic sensors may be attached to the sensor node to measure properties of the environment. Since the sensor nodes have limited memory and are typically deployed in difficult-to-access locations, a radio is implemented for wireless communication totransfer the data to a base station (e.g., a laptop, a personal handheld device, or an access point to a fixed infrastructure). Battery is the main power source in a sensor node. Secondary power supply that harvests power from the environment such as solar panels may be added to the node depending on the appropriateness of the environment where the sensor will be deployed. Depending on the application and the type of sensors used, actuators may be incorporated in the sensors [1].

Wireless sensor network is a self-configuring network of small sensor nodes which communicates with each other using radio signals. WSN joins together sensing, computation and communication in a single device called as sensor nodes. Wireless sensor nodes are also called as motes. In WSN, sensor nodes are used to send packets to a base station with the help of multi-hop transmission. Sensor nodes are classified into clusters and each of these clusters has a cluster head, it's shown in Fig1. Through cluster heads, Sensor nodes communicate data to the base station by combining data from its members [2].

Wireless Sensor Networks are used in ocean and wildlife monitoring, manufacturing machinery performance monitoring, building safety and earthquake monitoring, vehicular movement etc. Due toresource constraints of energy and memory, the conventional security measures are not suitable to these wireless sensor networks. An adversary can compromise a sensor node, it alters the integrity of the data, eavesdrop on messages, inject fake messages, and waste network resources. Unlike wired networks, wireless nodes