Detecting False Data in Wireless Sensor Network using Efficient Becan Scheme

Abstract

Wireless sensor networks (WSNs), as an emerging technology face numerous challenges. Sensor nodes are usually resource constrained and also vulnerable to physical attacks or node compromises. As the projected applications for wireless sensor networks range from smart applications such as traffic monitoring to critical military applications such as measuring levels of gas concentration in battle fields, security in sensor networks becomes a prime concern. In sensitive applications, it becomes imperative to continuously monitor the transient state of the system rather than steady state observations and take requisite preventive and corrective actions. Generally, the networks are prone to be attacked by adversaries who intend to disrupt the functioning of the system by compromising the sensor nodes and injecting false data into the network. So it is important to shield the sensor network from false data injection attacks. In this work, it is proposed to use a novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data based on Bloom Filter.

References

Detecting False Data in Wireless Sensor Network using Efficient Becan Scheme

Detecting False Data in Wireless Sensor Network using Efficient Becan Scheme


**Index Terms**

Computer Science Wireless

**Keywords**

Wireless Sensor Networks Bandwidth Injecting False Data Attack Bloom Filter