

## ETSNS00014 - Data Collection for Security Measurement in Wireless Sensor Networks

### Abstract

Wireless Sensor Network (WSN) is an indispensable part of IoT that has been applied in many fields to monitor environments and collect data from surroundings. However, WSNs are highly susceptible to attacks due to its unique characteristics: large-scale, self-organization, dynamic topology and constrained resources. A number of systems have been proposed to effectively detect varieties of attacks in WSNs. However, most previous surveys on WSN attacks focus on detection methods for only one or two types of attacks and lack detailed performance analysis. Additionally, the literature lacks comprehensive studies on security-related data (in short security data) collection in WSNs. In this paper, we first provide an overview of WSNs and classify the attacks in WSNs based on protocol stack layers. For the purpose of WSN security measurement, we then research attack detection methods of eleven mainstream attacks. We extract security data that play an important role for detecting security anomaly towards security measurement. We further elaborate the advantages and disadvantages of the existing detection methods based on a number of evaluation criteria. Finally, we highlight a number of open problems in this research field based on our thorough survey and conclude this paper with possible future research directions.

**Index Terms** — attack detection, Internet of Things (IoT), security data collection, security measurement, Wireless Sensor Network (WSN)



Maruthi Plaza 91/6, TC Palya Main road,  
Next to RK Apartments, Ramamoorthy Nagar,  
Bangalore-560025.



9543218650



ieeeprojects@eminent.in