Abstract

The potential use of wireless sensor networks (WSNs) in many technological situations is extensive. WSNs are employed in numerous areas, such as battlefields, traffic surveillance, healthcare, and environmental monitoring. Many studies have been conducted to improve various aspects of the performance of WSNs, such as energy efficiency, quality of service (QoS), reliability, mobility, scalability, and extended network lifetime. However, few studies have sought to advance the security of WSNs by focusing on medium access control (MAC), physical, and transport stacks. The network layer is the middle layer that coordinates the lower layers and the upper layers. Thus, the network layer is of paramount significance to the security of WSNs to prevent exploitation of their confidentiality, privacy, availability, integrity, and authenticity. The objective of this study is to address the security laps of WSNs on the network layer, particularly selective forwarding attacks. This paper includes a survey performed from 2003 to 2014. Significant constraints and hazards of physical attacks at the network layer are extensively addressed. The survey includes a benchmark for the comparison of existing approaches for handling the security of WSNs on the network layer and their challenges. Future directions are also comprehensively highlighted in the document. This study will help researchers to understand attacks on the network layer.
Comparative Analysis of Selective Forwarding Attacks over Wireless Sensor Networks

References

Comparative Analysis of Selective Forwarding Attacks over Wireless Sensor Networks

- J. Polastre, J. Hill, and D. Culler, "Versatile Low Power Media Access for
Comparative Analysis of Selective Forwarding Attacks over Wireless Sensor Networks

- Y. W. Law, S. Dulman, S. Etalle, P. Havinga, ”Accessing security-critical energy efficient sensor networks”; University of Twente, EA Enschede, Netherlands.  

**Index Terms**

Computer Science Wireless

**Keywords**

Wireless sensor network selective forwarding and denial of services attacks.