

Review of Wireless Sensor Network Security Schemes



Vaibhav D. Dabhade and A. S. Alvi

Abstract WSN is used in various applications such as hospital, environment monitoring, and experiments. It is also used in (military) [1, 2] battlefield for target tracking. If it is deployed in hostile environment in military application, then nodes can be captured and data can be updated. Wireless sensor network is equipped with low battery [3], storage, and computational power [4]. Hence, the main problem is the security of resource-constrained WSN. Various schemes are available to address the issues of WSN security. Proposed schemes are based on public and private encryption technique. Few schemes are based on biometric concept. While designing the security scheme researchers need to consider resource-constraint nature of wireless sensor network. Schemes are available but all are not applicable to WSN. This paper discusses various aspects of WSN to understand how schemes can be designed for WSN. Paper starts with application of WSN, summarizes security threats and analyzes various key management and security schemes.

Keywords Wireless sensor network security · Issues · Key management · Pairwise key generation

1 Introduction

A WSN is a group of spatially distributed autonomous devices, i.e., sensors. It can be used to monitor sound, temperature, vibration, pressure, motion, or pollutants [5]. Military application, such as battlefield surveillance [6, 7], is the main motivation for the work in WSNs. However, WSNs are now used in application areas such as industrial application, healthcare applications, environment, and habitat monitoring. In addition to these applications, nowadays, WSNs play an important role in traffic

V. D. Dabhade (✉)
Computer Engineering, MET's BKC, IOE, Nashik 422003, India
e-mail: vaibhavdabhade@rocketmail.com

A. S. Alvi
Information Technology, Prof. Ram Meghe Institute of Technology & Research, Badnera,
Amravati, India

© Springer Nature Singapore Pte Ltd. 2021
V. E. Balas et al. (eds.), *Intelligent Computing and Networking*,
Lecture Notes in Networks and Systems 146,
https://doi.org/10.1007/978-981-15-7421-4_4