22-23

Malicious Node Detection and Prevention for Secured Communication in WSN

Vaibhav Dabhade and A. S. Alvi

Abstract Wireless sensor networks (WSN) are composed primarily of resource-constrained sensor nodes, different monitoring characteristics and terminal nodes. Such types of infrastructure have been used in areas such as health care, defense, agricultural sectors, and emergency management, as communications systems and intrusion detection. Due to various growing use of wireless sensor networks, essential information is shared in an insecure channel among network entities including sensors, communication gateways, participants, etc., and the existence of critical and confidential information in the network emphasizes the difficulty of security risks. Through this work, we present the Hybrid Pairwise Key Establishment Scheme (HPKE) for connected devices with large scale sensors. This work often deals with the shortest path of computing among two nodes using broadcast tree construction (BTC) that optimizes the usage of internal resources and the consumption of energy. The intrusion detection scheme (IDS) recognizes certain possible factors of detecting malicious, potentially unreliable nodes during communication between nodes. Eventually, we will implement some dynamic application in network simulation environment of proposed system.

Keywords Wireless sensor network · BTC · Hybrid Pairwise Key Establishment Scheme

1 Introduction

A wireless sensor network (WSN) typically comprises several wireless small, low-power, and low-cost wireless network nodes. Every sensor node is powered by a

V. Dabhade (✉)
Computer Engineering, MET's BKC, IOE, Nashik, India
e-mail: vaibhavd_ioe@bkc.met.edu

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

A. P. Pandian et al. (eds.), *Computer Networks, Big Data and IoT*, Lecture Notes on Data Engineering and Communications Technologies 117,
https://doi.org/10.1007/978-981-19-0898-9_10