An Energy efficient approach for Secure data communication using Pairwise key encryptionin WSN

Vaibhav Dabhade[1], Dr. A.S. Alvi[2]

[1]MET's BKC of Institute Engineering, Nashik

[2]Prof. Ram Meghe Institute of Technology & Research, Amravati, India

Corresponding Author: vaibhavdabhade@rocketmail.com

Abstract:

A WSN is a wireless network comprising small sensor nodes to monitor environmental or physical parameters. Since wireless sensor networks have limited computational power, memory, throughput, and energy, traditional security solutions designed for resource-rich systems are inappropriate. Given these limitations, providing basic security methods for data transfer in wireless sensor networks is vital. Our work is divided in three phases. Phase 1 focuses on development of a pairwise key management technique. We suggested broadcast tree construction for a wireless sensor network in phase 2. In phase 3, we proposed an enhanced watchdog strategy as a practical way of detecting rogue nodes. The main objective of this model's depiction is to emphasize how important it is to reduce network power consumption to prolong network lifespan and identify and terminate rogue nodes before they broadcast packets. Experimental analysis shows that our model provides better results than state of art systems.

Keywords: lightweight key encryption, pairwise key generation, wireless sensor network, intrusion detection system, energy consumption and conservation, broadcast tree construction.

DOI Number: 10.48047/NQ.2022.20.15.NQ88632 **NeuroQuantology2022;20(15): 6311-6321**

1. Introduction

Due to recent advancements in compact microprocessors, low-power circuit designs, and radio methods, a new technological vision known as "Wireless Sensor Networks (WSNs)" is now practical. WSNs generally comprise of sensor nodes, combined with one or more sinks (base stations) or a network of sinks. The sensor nodes are equipped with low-cost sensing electronics, a small CPU, and a battery-operated device. Although the price and size of sensors vary based on the application, a fundamental sensor has a price of under $1 USD and a size of several cubic millimetres. When numerous sensors are scattered over a physical space, they form a special sort of connection that acts as a gateway to distant end users. Sinks act as this connection's gateways. One of the typical tasks for WSNs may be to detect or observe naturally occurring phenomena from the environment, such as heat, light, pressure, rays, pollution [1] etc. The sensor nodes provide the sink with either raw data or aggregated data. The sink makes decisions based on the combined data and is able to direct the network to allocate tasks to the sensors. In addition to several basic security flaws, wireless sensor nodes are further vulnerable since they are often deployed in unsupervised locations and depend on subpar radio communication. As a consequence of several assaults, end users can get erroneous sensing data, which might be detrimental in circumstances like battle monitoring and environmental monitoring. Appropriate security measures must be put in place to keep systems secure.The proposed pairwise key encryption and watchdog operates to identify and stop malicious nodesautomatically before it gets compromised while transferring data. The system may also enable secure communication while detecting several