Chapter 7
Wireless Sensor Networks and Communication Protocols

Mohammad Jeelani
Future University, India

Mohd Muqeem
Sandip University, India

Sultan Ahmad
https://orcid.org/0000-0002-3198-7974
Prince Sattam Bin Abdulaziz University, Alkharj, Saudi Arabia & Chandigarh University, Mohali, India

Aasim Zafar
https://orcid.org/0000-0003-1331-014X
Aligarh Muslim University, India

Mourade Azrour
Faculty of Sciences and Technics, Moulay Ismail University of Meknes, Morocco

Kishan Pal Singh
https://orcid.org/0000-0002-4289-6875
FET, Mangalayatan University, India

ABSTRACT

Wireless sensor networks has the potential to completely change a number of industries, including smart cities, healthcare, industrial automation, and environmental monitoring. WSNs use wireless communication between spatially dispersed autonomous sensors to track environmental or physical parameters like motion, pressure, temperature, and humidity. In this paper, we propose the trust-based approach for changing nodes with energy (TBNE) model, a trust-based strategy in a wireless sensor network. TBNE locates the network's troublesome nodes. The structure enhances node performance based on the trust concept for secure communication in WSN. Using its wireless interface, the device records a physical event and sends it to a base station. When a base station and sensor node cannot communicate directly, hop-by-hop communication is needed. The proposed approach is in a wireless sensor network called the rust-based approach for varying nodes with energy (TBNE)

DOI: 10.4018/979-8-3373-0330-7.ch007

model. Moreover, these results are validated with two simulators for better findings.

1. INTRODUCTION

Sensor nodes, which are independent gadgets containing a microcontroller, radio, sensors, and a set of batteries, make up a wireless sensor network (WSN). The device records a physical event and transmits it to a base station via its wireless interface. When a base station and sensor node cannot communicate directly, hop-by-hop communication is needed. Since WSNs may be quickly deployed in an area without further investments in a cable installation, they are projected to be employed in various scenarios (for example, emergency response, wildlife monitoring, or battlefield monitoring). When energy resources are considered, the advantage changes into a disadvantage. There are only two AA batteries in a typical sensor node. Energy conservation becomes challenging when a WSN is presumed to be left unattended, which is a common scenario (Ahmed et al. 2015) and (asha et al. 2019).

(Ahmad et al 2015) and (Duan et al 2014) employ the trust and energy-aware routing protocol (TERP) and TSRF concepts, which are lightweight and highly resistant to a variety of threats. These outcomes are then contrasted with energy to determine the favorable outcome. The trust-based strategy for variable nodes with energy (TBNE) model is the method we suggest in a wireless sensor network, nonetheless, if we want more effective outcomes. Moreover, these results are validated with two simulators for better findings. Therefore, the proposed approach gives the appropriate results with the help of their simulation.

TBNE focuses on two critical aspects: trustworthiness and varying energy effectiveness, essential for WSNs operating in hostile environments prone to attacks(Ahmad et al 2020). TBNE guides sensor nodes to transmit packets along the shortest paths, considering both trust and energy levels of varying nodes within the network.

Many brand-new protocols that consider the characteristics of WSNs have been put forth, including required distribution, routing, and medium access control (MAC) protocols. Only a few of these, though, were tested on actual hardware. Compared to simulations, which offer a simple and relatively quick evaluation of proposals, testing becomes more time-consuming when a test has dozens or hundreds of sensor nodes. However, when realistic models are not employed, or they are not appropriately calibrated, the simulation results are erroneous (frequently, even deceptive).

One of the most popular evaluation approaches in the field of computer networks is, without a doubt, network simulation. It is frequently employed in creating new network protocols and communication architectures (Ahmad & Afzal, 2022). By defining the behavior of the network nodes and the communication channels, so-called network simulators enable one to model any computer network. For instance, a

GuideMe: A Complete System for Indoor Orientation and Guidance
Eirini Barri, Christos John Bouras, Apostolos Gkamasand Spyridon Aniceto Katsampiris Salgado (2020). *International Journal of Smart Sensor Technologies and Applications (pp. 36-53).*
www.irma-international.org/article/guideme/281602