JOURNAL OF SOUTHERN COMMUNICATION ENGINEERING
ISLAMIC AZAD UNIVERSITY BUSHEHR BRANCH
E-ISSN: 2980-9231
https://jce.bushehr.iau.ir
https://doi.org/...

Vol. x/ No. x/xxx

Research Article

Presenting an Attack-Resistant Communication Model for Secure Routing in Underwater Sensor Networks

Tayebeh Nourali Ahari [1] | Mehdi Sadeghzadeh [2]

[1] Department of IT Management, Faculty of Management and Economics, Science and Research Branch, Islamic Azad University, Tehran, Iran.
Ta.ahari@gmail.com

[2] Department of Computer, Faculty of Mechanics, Electricity, and Computers, Science and Research Branch, Islamic Azad University, Tehran, Iran.
Sadeghzadeh1999@gmail.com

Correspondence
Mehdi Sadeghzadeh, Associate Professor of Computer Department, Faculty of Mechanics, Electricity and Computers, Science and Research Branch, Islamic Azad University, Tehran, Iran.
Sadeghzadeh1999@gmail.com

Received: 14 April 2024
Revised: 17 August 2024
Accepted: 18 August 2024

Abstract

Underwater communication networks face various challenges including packet routing, signal interference, energy consumption, and potential network attacks. While routing protocols are designed to withstand common disturbances in underwater environments, they are not specifically crafted to counteract potential attacks and malicious behavior by neighboring nodes. The primary factors contributing to security threats in underwater wireless sensor networks (UWSNs) include limited power supply, restricted communication media, and harsh underwater communication conditions.Therefore, this research aims to provide a communication model that is resistant to secure routing attacks in underwater sensor networks. For this purpose, two models were considered for communication links between each pair of nodes. Scenario 1 is a basic distance-based model. In the second scenario, a probabilistic channel gain model was used between each pair of nodes. The simulation results include four steps: 1)secure neighbor discovery under wormhole attacks in underwater sensor networks, 2) initial path discovery process that selects the next reliable forwarding node to the sink node, 3) attack detection process while distributing data based on state information Nodes to detect Sybil attack (Sybil) and 4) safe path discovery is an alternative to detect malicious nodes, showed that the proposed scheme achieved a better success rate than the basic scheme and achieved lower mobility energy cost than the original method. It has achieved a comparable degree of success.

Keywords: Underwater Internet of Things, Safe Neighbor Discovery, Underwater Routing, Wormhole Attack.

Highlights

- Limitation of processing and communication capabilities in underwater Internet of Things.
- Simulation of guide signal transmission and neighbor table formation in two communication models.
- The proposed method demonstrated the highest network throughput compared to the basic method.

Citation: [in Persian].