SUBHOJIT GHIMIRE, 1912160
COMPUTER SCIENCE ENGINEERING
NIT SILCHAR

Abstract

Wireless Sensor Networks (WSNs) are widely used in various applications, and clustering-based protocols have been proposed to improve network efficiency. However, existing protocols such as LEACH (Low-Energy Adaptive Cluster Hierarchical) have limitations in selecting appropriate Cluster Heads (CHs), leading to energy imbalances and potential security risks. To address these issues, this study proposes an optimal Cluster Head Selection (CHS) model that maximizes energy efficiency and security in WSNs. The proposed model considers factors such as trust evaluation (direct and indirect), distance, security (risk level evaluation), energy, delay, and path reliability to choose the best CH. The study utilizes the Slime Wrap Food Update with Cat and Mouse Optimization (SWFU-CMO) approach to select the optimal CH. Simulation results demonstrate the effectiveness of the proposed approach in terms of residual energy, throughput, and delay. Overall, the proposed model provides a promising solution for improving energy efficiency and security in WSNs.

Introduction

Wireless Sensor Networks (WSNs) have become increasingly popular in various applications due to their ability to collect and transmit data from remote locations with low power consumption. Clustering-based routing protocols have been proposed to improve the energy efficiency and network lifetime of WSNs. However, existing protocols such as LEACH suffer from limitations in selecting appropriate Cluster Heads (CHs) and potential security risks associated with random CH selection. Therefore, this study proposes an energy-efficient, reliable, and secure clustering-based routing model for WSNs that incorporates a novel trust-based security framework. This proposed model aims to address the limitations of existing routing protocols and improve the network's energy consumption, reliability, and security.

The proposed model incorporates a trust-based mechanism with cluster heads, where each sensor node selects a CH based on its residual energy and trustworthiness. The CH aggregates and forwards the data to the base station, resulting in improved energy efficiency and reliability. To ensure network security, the proposed model includes a trust evaluation process based on direct and indirect trust, risk level evaluation, and distance. Furthermore, the model considers path reliability to determine the quality of the chosen cluster.

The proposed model was evaluated using NS2 simulation and compared with existing routing protocols. The simulation results demonstrate that the proposed model outperforms other routing protocols in terms of energy consumption, packet delivery ratio, and network lifetime. Additionally, the proposed security framework effectively detects and isolates malicious nodes, ensuring the network's security.

Paper Details	Methodology	Advantages	Disadvantages
Biradar, Mallanagouda & Mathapathi, Basavaraj. (2023). Energy, Reliability, and Trust-Based Security Framework for Clustering-Based Routing Model in WSN. International Journal of Information Security and Privacy. 17. 1-18. 10.4018/IJISP.315817.	Literature review Proposal of a new framework Performance evaluation Comparison with other models Analysis of results	Improved Energy Efficiency Enhanced Network Reliability Improved Network Security	Complexity Computational Overhead Limited Mobility

Brief Methodology

1. Literature review: Systematic search and analysis of existing literature on clustering-based routing models in WSNs. Review of literature on clustering-based routing models in wireless sensor networks (WSNs).

2. Proposal of a new framework: Identification of energy-efficient techniques, reliability measures, and trust-based security mechanisms based on the literature review; development of a new clustering-based routing model that incorporates these techniques and mechanisms. Proposal of a clustering-based routing model that incorporates energy-efficient techniques, reliability measures, and trust-based security mechanisms.

3. Performance evaluation: Implementation of the proposed framework in MATLAB; simulation of the framework in a WSN environment with varying numbers of nodes and network densities. Performance evaluation of the proposed framework using simulations in MATLAB.

4. Comparison with other models: Implementation of LEACH and TEEN in MATLAB; simulation of these models in the same WSN environment as the proposed framework. Comparison of the proposed framework with two other clustering-based routing models: LEACH and TEEN.

5. Analysis of results: Collection and analysis of simulation results in terms of energy efficiency, reliability, and security; discussion of the performance of the proposed framework compared to LEACH and TEEN. Analysis of simulation results and discussion of the performance of the proposed framework in terms of energy efficiency, reliability, and security.

Tables and Charts: Overall performances of SWFU-CMO model over existing models

Table 1: Alive Nodes

No. of Nodes	No. of Round	FPU-DA	DMEERP	CMBO	SMA	GOA	ALO	SGO	RHSO	SWFU-CMO
50	**2000**	3.000	1.878	1.606	1.400	1.366	1.220	2.000	3.000	6.000
100	**2000**	19.000	13.794	13.074	13.074	11.864	11.764	15.000	18.000	21.000
150	**2000**	40.000	31.708	31.063	26.884	23.413	22.795	32.000	37.000	42.000

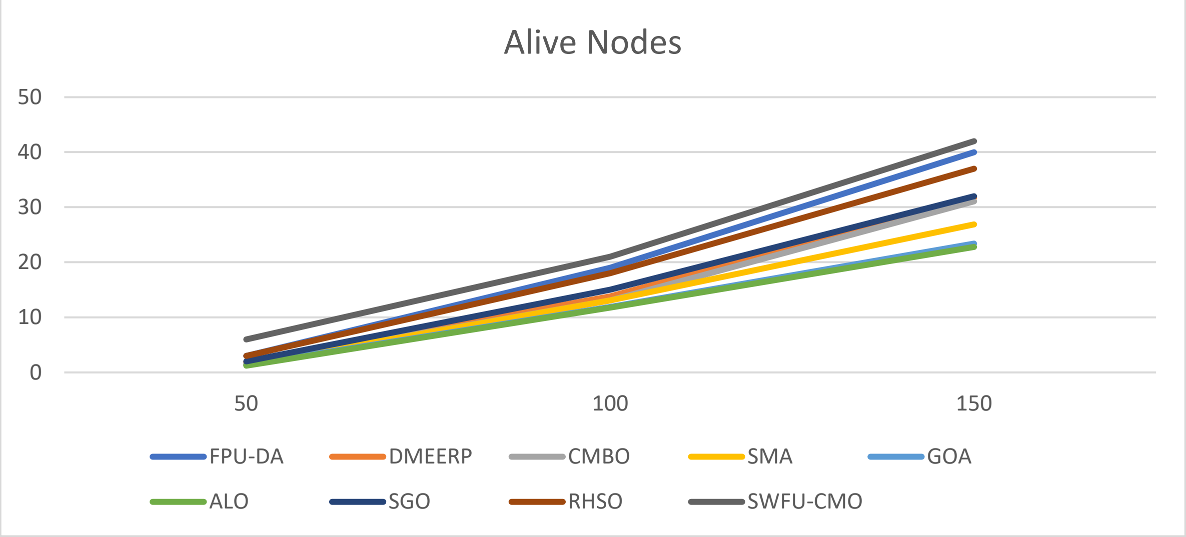


Table 2: Delay

No. of Nodes	No. of Round	FPU-DA	DMEERP	CMBO	SMA	GOA	ALO	SGO	RHSO	SWFU-CMO
50	**2000**	0.599	0.813	0.835	0.836	1.202	1.700	0.599	0.599	0.549
100	**2000**	0.650	0.958	1.011	1.122	1.254	1.299	0.843	0.765	0.539
150	**2000**	0.599	0.875	0.940	1.398	1.451	1.674	0.829	0.635	0.539

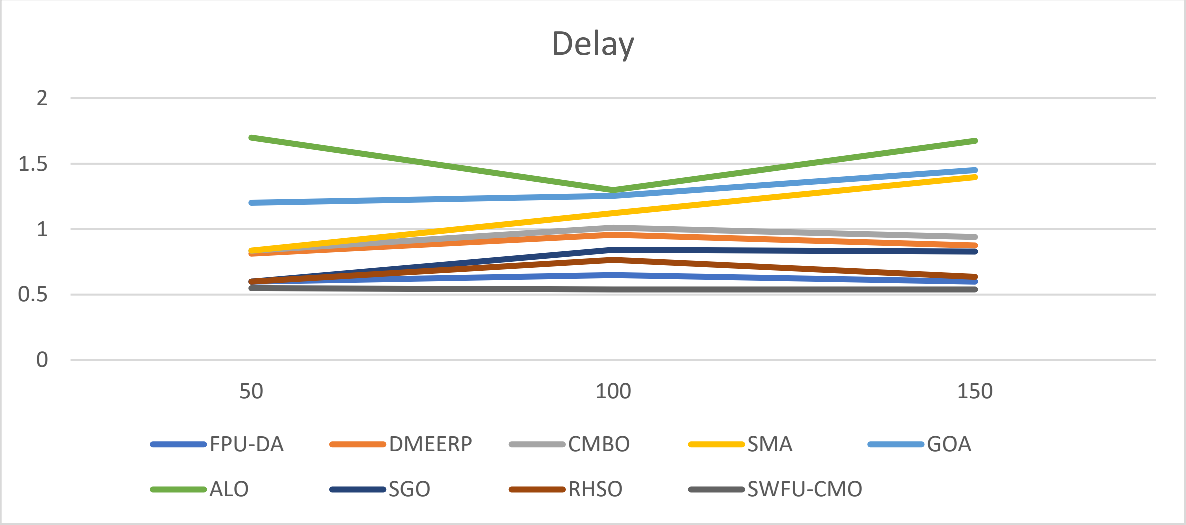


Table 3: Average Residual Energy

No. of Nodes	No. of Round	FPU-DA	DMEERP	CMBO	SMA	GOA	ALO	SGO	RHSO	SWFU-CMO
50	**2000**	0.731	0.920	0.935	1.070	1.327	1.317	0.647	0.648	1.554
100	**2000**	1.250	1.253	1.448	1.537	1.860	1.855	0.366	1.372	2.168
150	**2000**	2.549	2.361	2.573	2.609	2.695	2.691	1.161	2.558	3.427

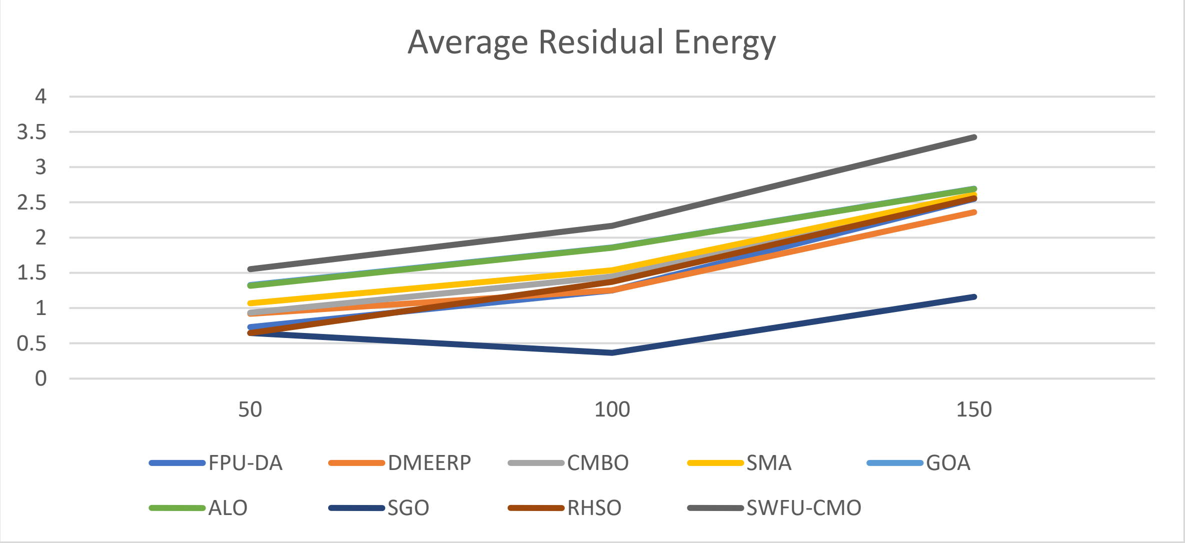
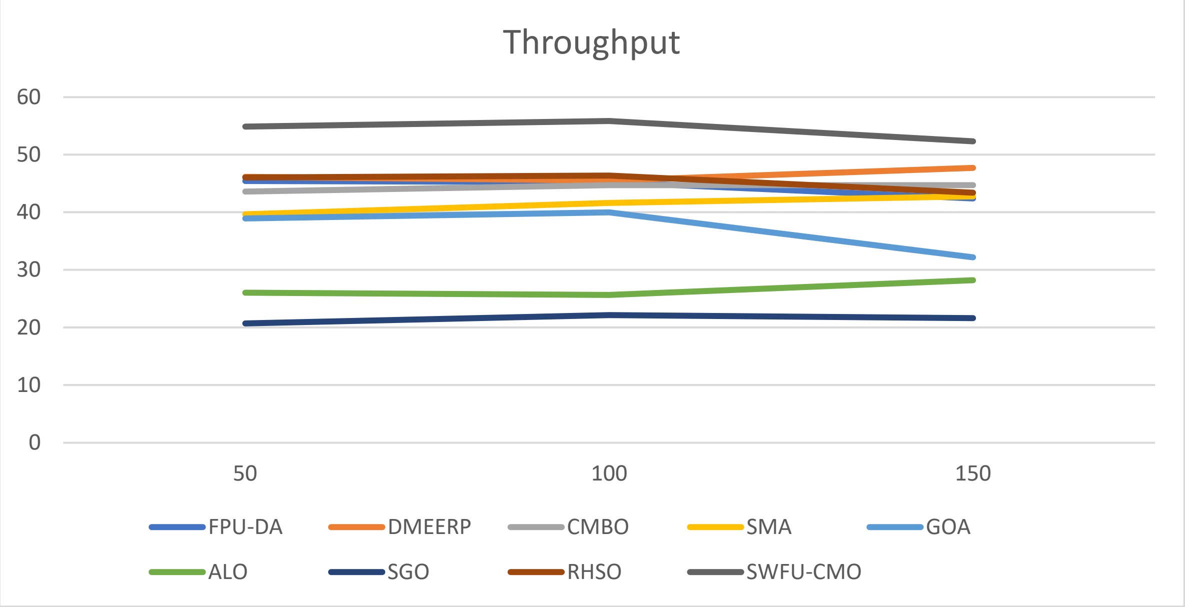


Table 4: Throughput

No. of Nodes	No. of Round	FPU-DA	DMEERP	CMBO	SMA	GOA	ALO	SGO	RHSO	SWFU-CMO
50	**2000**	45.423	46.153	43.603	39.657	38.908	26.036	20.717	46.025	54.869
100	**2000**	45.219	45.525	44.709	41.625	39.999	25.660	22.150	46.381	55.855
150	**2000**	42.413	47.699	44.699	42.752	32.176	28.198	21.609	43.397	52.330



Conclusion

This study proposed an energy-efficient, reliable, and secure clustering-based routing model for WSNs that incorporates a trust-based security framework. The proposed model addressed the limitations of existing routing protocols and improved the network's energy consumption, reliability, and security. The proposed model incorporated a trust-based mechanism with cluster heads, where each sensor node selected a CH based on its residual energy and trustworthiness. The CH aggregated and forwarded the data to the base station, resulting in improved energy efficiency and reliability. The proposed security framework effectively detected and isolated malicious nodes, ensuring the network's security. The simulation results demonstrated the effectiveness of the proposed approach in terms of residual energy, throughput, and delay. Overall, the proposed model provides a promising solution for improving energy efficiency and security in WSNs, which can be applied in various applications, including environmental monitoring, healthcare, and smart cities. Future work may involve further optimization of the proposed model, such as investigating the impact of different trust evaluation mechanisms and considering the effect of mobility and node failure.

Bibliography

Biradar, Mallanagouda & Mathapathi, Basavaraj. (2023). Energy, Reliability, and Trust-Based Security Framework for Clustering-Based Routing Model in WSN. International Journal of Information Security and Privacy. 17. 1-18. 10.4018/IJISP.315817.

BibTex:

```
@article{article,
author = {Biradar, Mallanagouda and Mathapathi, Basavaraj},
year = {2023},
month = {01},
pages = {1-18},
title = {Energy, Reliability, and Trust-Based Security Framework for Clustering-Based Routing Model in WSN},
volume = {17},
journal = {International Journal of Information Security and Privacy},
doi = {10.4018/IJISP.315817}
}
```

Author: Mallanagouda Biradar and Basavaraj Mathapathi
Paper Title: Energy, Reliability, and Trust-Based Security Framework for Clustering-Based Routing Model in WSN
Published In peer-reviewed academic journal: International Journal of Information Security and Privacy
Featured Pages: pages 1-18, Volume 17