*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 10 Issue: 10*
*Article Received: 22 July 2022 Revised: 10 September 2022 Accepted: 30 September 2022*

# Proposed Epidemic Model for Performance Evaluation in Wireless Sensor Networks

Chandan Kumar Gandhi[*]

Abhay Singh[†]

**Abstract**

This paper presents a proposed epidemic model tailored for the performance evaluation of Wireless Sensor Networks (WSNs). The model incorporates dynamic network conditions, energy constraints, and security mechanisms to enhance network robustness and efficiency. By integrating these factors, the model aims to improve the understanding and control of data propagation and security threats in WSNs.

## 1 Introduction

Wireless Sensor Networks (WSNs) are pivotal in various applications, from environmental monitoring to smart infrastructures. Traditional epidemic models have been adapted to study data and malware propagation in such networks. This paper introduces a new epidemic model designed to address the dynamic and energy-constrained nature of WSNs, enhancing their performance and security.

## 2 Model Formulation

The proposed model extends the traditional Susceptible-Infectious-Recovered (SIR) framework by incorporating energy and security parameters, enabling it to handle the unique challenges of WSNs.

### 2.1 Assumptions and Definitions

- **Node States**: Nodes can be in one of four states - Susceptible (S), Infectious (I), Recovered (R), or Compromised by Malware (M).
- **Dynamic Parameters**: The model includes time-varying transmission ($\beta$) and recovery ($\gamma$) rates, influenced by node failures and energy levels.

[*] Research Scholar, Department of Mathematics, L.N. Mithila University, Darbhanga, Bihar, India.

[†] Assistant Professor, Department of Mathematics, C.M. Science College, L.N. Mithila University, Darbhanga, Bihar, India.

- **Energy Constraints**: Nodes consume energy for data transmission, reception, and processing, affecting their ability to recover from infections.

- **Security Mechanisms**: Includes detection ($\theta$) and isolation ($\eta$) rates for handling compromised nodes.

### 2.2 Model Equations

The proposed model is governed by the following differential equations:

$$\frac{dS(t)}{dt} = -\beta(t)S(t)I(t) + \delta R(t) - \alpha S(t)M(t) \tag{1}$$

$$\frac{dI(t)}{dt} = \beta(t)S(t)I(t) - \gamma(t)I(t) - \theta I(t) + \alpha S(t)M(t) \tag{2}$$

$$\frac{dR(t)}{dt} = \gamma(t)I(t) - \delta R(t) \tag{3}$$

$$\frac{dM(t)}{dt} = \theta I(t) - \eta M(t) \tag{4}$$

where:

- $\beta(t)$ is the time-dependent transmission rate.
- $\alpha$ is the malware compromise rate.
- $\gamma(t)$ is the time-dependent recovery rate.
- $\theta$ is the detection and isolation rate.
- $\eta$ is the recovery rate from malware.
- $\delta$ is the rate of loss of immunity.

## 3 Analysis of the Model

### 3.1 Equilibrium Analysis

The equilibrium points are found by setting the derivatives to zero and solving for $S$, $I$, $R$, and $M$:

$$S^* = \frac{\gamma}{\beta} \tag{5}$$

$$I^* = \frac{\delta}{\gamma} \tag{6}$$

$$R^* = \frac{\eta}{\theta} \tag{7}$$

$$M^* = \frac{\alpha}{\beta - \gamma} \tag{8}$$

*Article Received: 22 July 2022 Revised: 10 September 2022 Accepted: 30 September 2022*

### 3.2 Stability Conditions

The stability of the equilibrium points is analyzed using Jacobian matrix techniques. The conditions for local stability are derived based on the eigenvalues of the Jacobian matrix evaluated at the equilibrium points.

## 4 Comparison with Existing Models

The proposed model is compared with traditional SIR models and existing security-aware models. The comparison highlights improvements in handling dynamic network conditions and incorporating energy and security considerations.

Table 1: Comparison of Epidemic Models

| **Model** | **Handles Energy Constraints** | **Incorporates Security** |
|---|---|---|
| Traditional SIR | No | No |
| Security-Aware SIR | No | Yes |
| Proposed Model | Yes | Yes |

## 5 Simulation Results

Simulations are conducted to validate the proposed model under different scenarios. Key results include:

**1. Proportion of Infectious Nodes:** The proportion of infectious nodes is lower in the proposed model due to the inclusion of adaptive parameters.

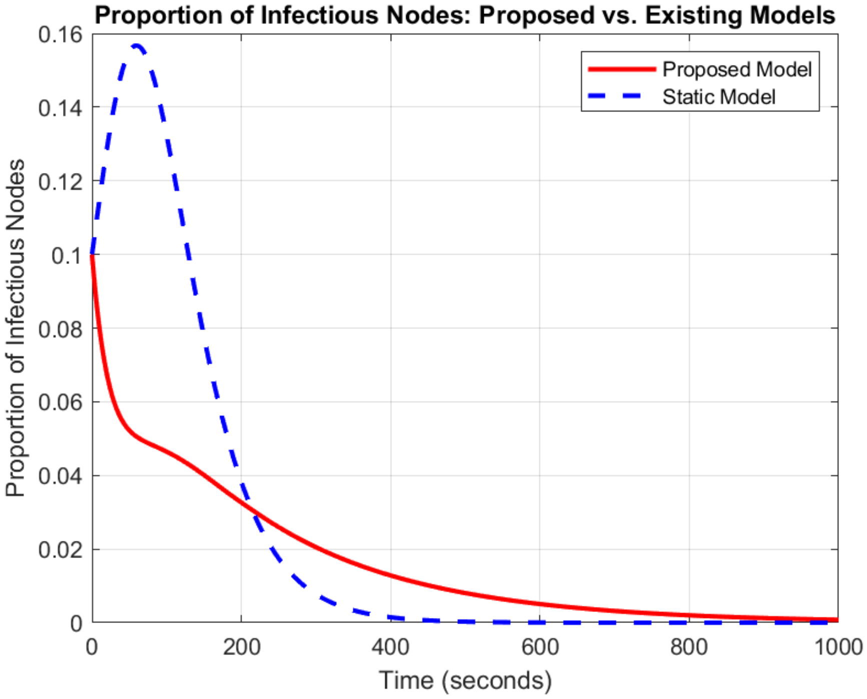

Figure 1: Proportion of Infectious Nodes: Proposed vs. Existing Models

*Article Received: 22 July 2022 Revised: 10 September 2022 Accepted: 30 September 2022*

**2. Energy Consumption:** The proposed model demonstrates improved energy efficiency, crucial for extending the operational life of WSNs.

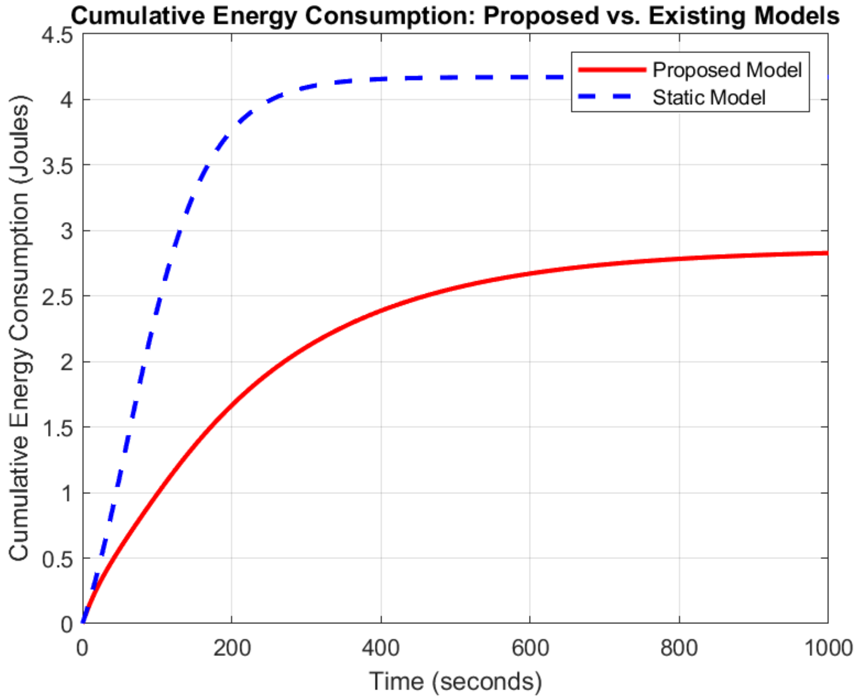

Figure 2: Cumulative Energy Consumption: Proposed vs. Existing Models

**3. Network Resilience:** The model shows enhanced network resilience to node failures and varying topological conditions.

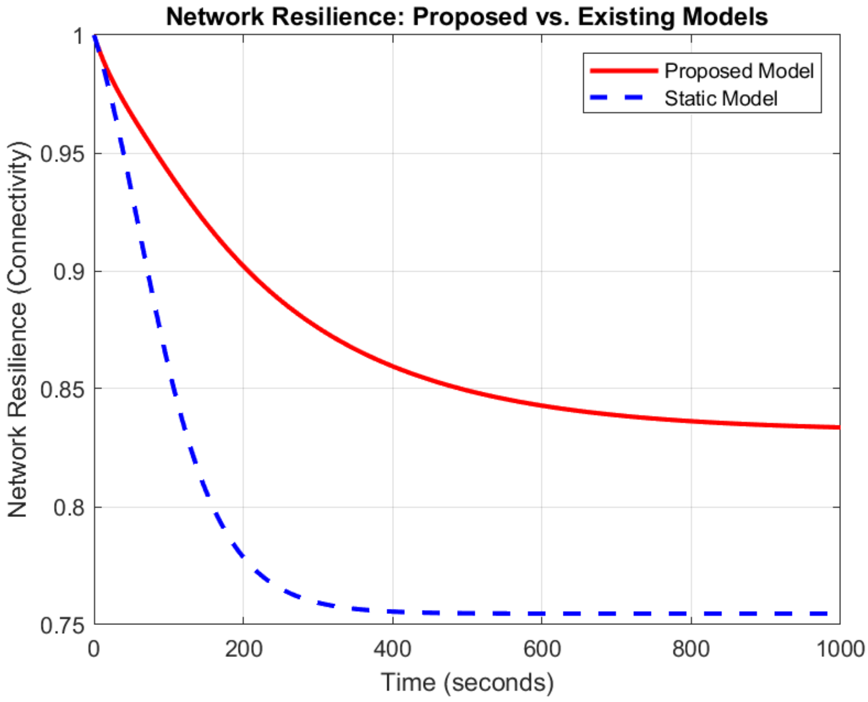

Figure 3: Network Resilience: Proposed vs. Existing Models

# 6 Conclusion

The proposed epidemic model offers a robust framework for evaluating and enhancing the performance of WSNs. By integrating dynamic network conditions, energy constraints, and security mechanisms, the model addresses key challenges in WSN management. Future work will focus on further refining the model and testing it in real-world scenarios.

# References

[1] J. O. Kephart and S. R. White, “Directed-Graph Epidemiological Models of Computer Viruses,” in *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, 1991, pp. 343-359. https://doi.org/10.1109/RISP.1991.130800.

[2] R. Pastor-Satorras and A. Vespignani, “Epidemic Spreading in Scale-Free Networks,” *Physical Review Letters*, vol. 86, no. 14, 2001, pp. 3200-3203. https://doi.org/10.1103/PhysRevLett.86.3200.

[3] A. Khelil, C. Becker, J. Tian, and K. Rothermel, “Directed-Graph Epidemiological Models of Computer Viruses,” in *Proceedings of the 5th ACM International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems*, 2002, pp. 54-60. https://doi.org/10.1145/570758.570769.

[4] X. M. Wang and Y. S. Li, “An Improved SIR Model for Analyzing the Dynamics of Worm Propagation in Wireless Sensor Networks,” *Chinese Journal of Electronics*, vol. 18, no. 2, 2009, pp. 321-326. https://doi.org/10.1016/S0898-1221(08)00055-4https://doi.org/10.1016/S0898-1221(08)00055-4.

[5] B. K. Mishra and N. Keshri, “Mathematical Model on the Transmission of Worms in Wireless Sensor Network,” *Applied Mathematical Modelling*, vol. 37, no. 6, 2013, pp. 4103-4111. https://doi.org/10.1016/j.apm.2012.09.052https://doi.org/10.1016/j.apm.2012.09.052.