Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 17** : 1–13.
ISSN-0037-8712
doi:10.5269/bspm.82697

Securing Medical IoT Devices: A Time-Delay Mathematical Approach for Cyber-Attack Detection and Mitigation

Pankaj Kumar*, Pankaj Rai, Bimal Kumar Mishra

ABSTRACT: Medical Internet of Things (MIoT) systems operate under strict latency constraints, where even brief delays in communication or cyber-incident response can significantly worsen malware spread and disrupt clinical services. This study proposes a time-delay differential equation (TDDE) model that explicitly accounts for propagation delay (τ_1) and mitigation response delay (τ_2) in MIoT networks, allowing delay-induced instability to be examined directly. Devices are classified into secure, compromised, and recovered states. Analytical investigation establishes the malware-free equilibrium, endemic equilibrium, and a delay-adjusted basic reproduction number R_0. The analysis reveals a clear threshold structure: when $R_0 < 1$, malware dies out and the system converges to a stable state, whereas $R_0 > 1$ leads to sustained compromise.

Numerical simulations support these findings. Minor delays result in smooth, controlled infection trajectories, while larger delays trigger oscillatory outbreaks and prolonged system degradation. Sensitivity analysis identifies infection rate, recovery effectiveness, and device turnover as key drivers of system behavior, with delays significantly amplifying their impact. These results highlight the necessity of delay-aware modeling for designing resilient MIoT cybersecurity mechanisms capable of supporting uninterrupted clinical operations. The current framework assumes homogeneous devices and fixed delays; future work should extend the model to heterogeneous network structures, time-varying delays, and hybrid TDDE–machine learning defense strategies.

Keywords: Medical Internet of Things (MIoT), Time-Delay Differential Equations (TDDE), cyber-attack modeling, propagation and response delays, stability analysis, reproduction number R_0, malware dynamics.

Contents

* Corresponding author.
2020 *Mathematics Subject Classification:* 34K20, 34K13, 92C42, 68T07, 68M15.
Submitted March 14, 2026. Published June 19, 2026.

1. Introduction

The rapid expansion of Internet of Things (IoT) technologies across healthcare has reshaped clinical workflows, diagnostics, and real-time patient monitoring. Medical IoT (MIoT) devices now form the backbone of many critical systems, but their reliance on continuous connectivity and low-latency communication exposes them to significant cybersecurity risks. These devices often operate with limited computational capacity, rely heavily on wireless communication, and handle sensitive clinical data. A successful cyber-attack in this environment can compromise privacy, disrupt essential medical functions, and threaten patient safety. Conventional cybersecurity models, many of which are based on ordinary differential equations (ODEs), struggle to represent the complex behavior of cyber threats within MIoT networks. They assume instantaneous interactions and fail to account for the delays that naturally arise in real systems. In practice, malware propagation is shaped by communication latency, device processing time, and the lag between detecting an intrusion and deploying a response. Ignoring these delays oversimplifies system dynamics and leads to incomplete or misleading predictions about how attacks evolve. To address these limitations, this study introduces a defense model built on Time-Delay Differential Equations (TDDEs). The model incorporates two critical delays: the time required for an infection to propagate across the network and the lag between detection and recovery. This delay-aware structure captures the true temporal nature of MIoT cyberattacks and provides a more accurate description of infection spread and recovery behavior. The analysis proceeds by examining equilibrium conditions, characterizing system stability, and identifying the basic reproduction number that governs long-term behavior. Numerical simulations further show how different delay values shape infection dynamics. Together, the theoretical and empirical results highlight the importance of accounting for delays when designing security protocols and planning mitigation strategies in MIoT environments.

2. Literature Review

The growth of Medical IoT (MIoT) has expanded the digital boundary of healthcare, but it has also introduced complex security challenges driven by device heterogeneity, latency constraints, and continuous data exchange. [1] underscored that many MIoT devices are deployed with minimal authentication and weak encryption, creating an environment where attacks such as spoofing, tampering, and unauthorized access can compromise clinical workflows and patient safety. Their analysis highlights the fragility of many healthcare deployments and sets the stage for understanding why dynamic, system-level threat models are essential. Machine learning-driven detection systems have emerged as a major defense avenue. [2] demonstrated that ensemble learning techniques can significantly improve the identification of denial-of-service and delay-based attacks within IoMT networks. [8] further showed that anomaly detection models, especially those relying on neural networks, are capable of flagging previously unseen threat behaviors in real time. Complementing these findings, [10] emphasized that ML-based risk mitigation frameworks remain central to managing vulnerabilities in healthcare IoT systems, although their performance is often limited by system latency and inconsistent device behavior. Delay-induced instability is another major theme in cyber–physical security research. [3] illustrated how even small delays in feedback-driven systems can trigger oscillations or chaotic responses, a phenomenon highly relevant to MIoT networks where response lag is common. In the cybersecurity domain, [4] analyzed a delayed SEI2RS malware propagation model and showed that incorporating time lags fundamentally alters the infection threshold and stability landscape. Similar behavior was observed by [13], whose virus model demonstrated that multiple transmission pathways combined with delays can foster persistent infections. These insights directly support the need for time-delay differential equation (TDDE) models in understanding MIoT cyberattacks. Several recent works have explored time-delay modeling within industrial and IoT infrastructures. [7] examined systems with dual delays and nonlinear infection rates, showing that minor variations in delay values can shift system equilibrium dramatically. [15] also established how delay-induced switching behavior emerges in slow–fast dynamical systems, further reinforcing the argument that delay-aware modeling provides a more faithful representation of cyber–physical behavior. On the methodological side, [16] highlighted accuracy and stability concerns in numerical solutions of delayed differential equations, guidance essential for implementing reliable simulation frameworks. More advanced perspectives, such as fractional time-delayed dynamics explored by [14], reveal additional modeling flexibility for systems with memory-dependent be-

havior. Security mechanisms developed for IoT and industrial environments offer relevant architectural perspectives. [5] proposed a lightweight authentication mechanism combining elliptic curve cryptography with trusted tokens, demonstrating that efficient cryptographic design can reduce latency without weakening security. [6] introduced a hybrid fog–edge architecture for IoMT applications, emphasizing that proximity-based computation enhances both response time and resilience during attacks. These architectural approaches align with the broader argument that delay minimization is fundamental for maintaining MIoT stability. Beyond direct modeling and authentication, system-level frameworks offer structured guidance for secure MIoT deployment. The IoT Security Institute [9] recommended incorporating formal threat models during device design, accounting for communication, trust evaluation, and risk propagation paths. [12] reviewed existing MIoT security frameworks and highlighted gaps in risk assessment methodologies, particularly in handling time-sensitive threats and distributed decision-making. [11] added to this perspective by summarizing how time-series analysis supports intrusion detection and attack prediction, suggesting that predictive analytics can complement mathematical models in reducing detection delays. Research in related IoT and networked systems also informs MIoT cybersecurity. [17] discussed optimizing sensor network longevity through improved routing and sink placement, demonstrating how system design decisions affect resilience and communication delays. [18] explored fractional virus propagation models, signaling broader applicability of mathematical epidemic frameworks in cyber-threat analysis. Recent domain-specific contributions further reinforce the importance of dynamic risk modeling. [19] developed a deep learning-based intrusion detection system for smart cars, showing that mobility-intensive IoT environments face similar latency and propagation challenges. [20] proposed the SEQIRE model for attack detection in IoT networks, demonstrating how multi-compartment mathematical structures can capture infection and recovery phases with greater precision. These works align closely with the motivation of the present study, especially in highlighting the value of mathematically grounded cybersecurity modeling. Together, these studies reveal a consistent narrative: MIoT security cannot be understood without accounting for delays in propagation, detection, and response. Existing literature strongly supports the integration of TDDE-based approaches to capture these dynamics and underscores the need for models that reflect both the temporal and structural complexity of healthcare-connected devices.

3. Mathematical Modelling

Time-Delay Differential Equations (TDDEs) extend ordinary differential equations by incorporating delays that influence system behavior. Because MIoT devices experience communication lag, delayed detection, and delayed recovery, TDDEs provide a natural mathematical foundation for studying cyber-attack dynamics [14].

3.1. Assumptions and Model Components

The model begins with a set of structural assumptions describing how MIoT devices behave under cyber-attack. The network is considered homogeneous, meaning all devices share similar vulnerability levels and follow comparable infection and recovery patterns. Device recruitment and removal occur at constant rates, reflecting regular deployment and retirement in healthcare environments. Two delays are central to the model: Propagation delay $(\tau - 1)$: the time taken for malware to spread from compromised devices to secure ones. Response delay (τ_2): the lag between identifying a compromised device and initiating its recovery. These assumptions simplify the system while capturing the essential timing behavior that influences malware spread and mitigation in real MIoT networks.

3.2. Hypothesis

The core hypothesis guiding the model is that delays in propagation and response significantly alter infection dynamics, potentially destabilizing the system even when infection rates are moderate. Delays may increase outbreak peaks, prolong infection periods, or shift the network from stable to oscillatory behavior. Therefore, including τ_1 and τ_2 in the equations should provide a more realistic and sensitive representation of MIoT cybersecurity conditions than delay-free ODE models.

3.3. Model Definition

The system divides devices into three functional categories:

- S(t): Secure devices not currently infected
- I(t): Compromised devices affected by cyber-attacks
- R(t): Recovered devices restored to secure operation

The transitions between these states are governed by:

- α : recruitment rate
- β : infection transmission rate
- γ : recovery rate
- μ : natural removal rate
- τ_1: malware propagation delay
- τ_2 : recovery response delay

A standard TDDE takes the general form:

$$\frac{dx}{dt} = f\big(x(t), x(t-\tau)\big) \tag{3.1}$$

This structure allows present system behavior to depend on past states, capturing MIoT delays realistically. [4] [15].

3.4. Model Development Based on the Hypothesis

Building on the assumptions and hypothesis, the cyber-attack model is formulated with three TDDEs:

$$\frac{dS(t)}{dt} = \alpha - \beta S(t)I(t-\tau_1) - \mu S(t) \tag{3.2}$$

$$\frac{dI(t)}{dt} = \beta S(t)I(t-\tau_1) - \gamma I(t-\tau_2) - \mu I(t) \tag{3.3}$$

$$\frac{dR(t)}{dt} = \gamma I(t-\tau_2) - \mu R(t) \tag{3.4}$$

Here:

- Malware transmission depends on delayed infection terms $I(t-\tau_1)$.
- Recovery is initiated only after a response delay $I(t-\tau_2)$.
- Device removal affects all compartments equally.

This structure directly reflects the hypothesis: time delays influence not just the rate but the stability of infection dynamics.

3.5. Equilibrium and Reproduction Number Analysis

To understand the long-term behavior of the TDDE model, we examine the system's equilibrium points. At equilibrium, device populations no longer change with time, meaning the derivatives of all three state variables must equal zero. This allows us to characterize conditions under which malware dies out or persists within an MIoT network. The equilibrium states are obtained by setting the right-hand sides of the TDDE system to zero:

$$\frac{dS(t)}{dt} = \frac{dI(t)}{dt} = \frac{dR(t)}{dt} = 0 \tag{3.5}$$

Thus, the equilibrium conditions are:

$$\alpha - \beta S^* I^* - \mu S^* = 0 \tag{3.6}$$

$$\beta S^* I^* - \gamma I^* - \mu I^* = 0 \tag{3.7}$$

$$\gamma I^* - \mu R^* = 0 \tag{3.8}$$

where S^*, I^*, R^* denote equilibrium states. The system admits two biologically meaningful equilibria.

3.5.1. Malware-Free Equilibrium (MFE). At this equilibrium, $I^* = 0$, The secure device population balances recruitment and removal:

$$S^* = \tfrac{\alpha}{\mu}$$

This represents a fully secure MIoT network with no active infections.

3.5.2. Endemic Equilibrium (EE). In this case, $I^* > 0$, indicating persistent malware presence. This equilibrium reflects a scenario where infection continues despite recovery and removal processes.
Theorem 1: Existence of the Malware-Free Equilibrium To formalize the result above, we first establish the existence of the MFE. The malware-free equilibrium $E_0 = (\frac{\alpha}{\mu}, 0, 0)$ exists uniquely.
Proof: At MFE, $I^* = R^* = 0$. Substituting these into Eq. 3.6 gives:

$$\alpha - \mu S^* = 0 \Rightarrow S^* = \frac{\alpha}{\mu} \tag{3.9}$$

Since no infected or recovered population is present, the equilibrium is unique and well-defined.

Theorem 2: Basic Reproduction Number R_0 To determine whether infection can invade the MIoT network, we derive the basic reproduction number. The basic reproduction number for the TDDE model is:

$$R_0 = \frac{\beta S^* e^{-\mu\tau_1}}{\gamma + \mu} \tag{3.10}$$

This value represents the average number of secondary infections produced by a single compromised device in a fully secure network.
Proof: To derive R_0, we linearize the infection dynamics around the malware-free equilibrium

$$E_0 = (\tfrac{\alpha}{\mu}).$$

The infection equation becomes:

$$\frac{dI(t)}{dt} \approx \beta S^* I(t - \tau_1) - (\gamma + \mu) I(t) \tag{3.11}$$

Assume a trial solution of the form

$$I(t) = e^{\lambda t} \tag{3.12}$$

which gives the characteristic equation:

$$\lambda + (\gamma + \mu) = \beta S^* e^{\lambda \tau_1} \tag{3.13}$$

At the threshold of stability, set $\lambda = 0$, yielding:

$$\gamma + \mu = \beta S^* e^{\mu \tau_1} \tag{3.14}$$

Rearranging terms gives the basic reproduction number:

$$R_0 = \frac{\beta S^* e^{\mu \tau_1}}{\gamma + \mu} \tag{3.15}$$

This expression shows how the propagation delay τ_1 reduces infection strength through the decay factor $e^{-\mu \tau_1}$. If $R_0 < 1$, infection cannot sustain itself; if $R_0 > 1$, malware can persist.

3.6. Stability Analysis and Analytical Result

After establishing the basic reproduction number R_0, we evaluate how it governs the stability of both the malware-free equilibrium (MFE) and the endemic equilibrium (EE). This analysis clarifies whether infections die out or persist under different delay and parameter conditions.
The malware-free equilibrium $E_0 = (\frac{\alpha}{\mu}, 0, 0)$ is examined first.
Theorem 3: The malware-free equilibrium E_0 is locally asymptotically stable if and only if $R_0 < 1$ [15].
Proof: Substituting $I(t) = e^{\lambda t}$ into the linearized infection equation yields the characteristic form

$$\lambda + \gamma + \mu - \beta S_0 e^{-\lambda \tau_1} = 0.$$

Stability requires all eigenvalues λ to satisfy $\mathbb{R}(\lambda) < 0$. As $\lambda \to 0^-$, the inequality

$$\gamma + \mu > \beta S_0$$

follows, which is equivalent to

$$R_0 = \frac{\beta S_0 e^{-\mu \tau_1}}{\gamma + \mu} < 1.$$

Thus, when $R_0 < 1$, any initial infection decays, and the MIoT network naturally returns to a secure state. When $R_0 > 1$, infection may persist.
Theorem 4: If $R_0 > 1$, an endemic equilibrium $E^* = (S^*, I^*, R^*)$ with $I^* > 0$ exists and can be stable under appropriate parameter conditions [4].
Proof: Linearizing around E^* results in transcendental characteristic equations due to the presence of delays. Their stability cannot be determined analytically and is therefore assessed numerically. Using standard tools such as D-subdivision techniques or bifurcation analysis, stability is confirmed when all eigenvalues of the characteristic equation have negative real parts. Stability depends jointly on the infection rate β, recovery rate γ, removal rate μ, and both delays τ_1 and τ_2. Taken together, the analytical results yield a clear threshold behavior:

- If $R_0 < 1$, the malware-free equilibrium is stable and all infections eventually vanish.
- If $R_0 > 1$, the endemic equilibrium exists with persistent infection; its stability depends on system parameters and delay values.

These findings confirm the central role of time delays in shaping MIoT malware dynamics and demonstrate that propagation and response delays can determine whether an attack is naturally contained or evolves into a persistent threat.

4. Numerical Simulations and Validations

To validate the theoretical findings derived in the previous sections, numerical simulations of the proposed Time-Delay Differential Equation (TDDE) model were performed. Because the system exhibits nonlinear and delay-driven dynamics, the classical fourth-order Runge–Kutta (RK4) scheme is adapted to incorporate delayed state values. This approach provides the stability and accuracy necessary to replicate realistic Medical IoT (MIoT) cyber-attack behavior.

4.1. Numerical Method: Fourth-order Runge-Kutta (RK4)

The TDDE system was solved using the fourth-order Runge–Kutta method modified to handle the delayed terms. This method is well-established for nonlinear dynamical systems and remains one of the most reliable schemes for delay differential equations. Given the complexity introduced by the two delays τ_1 and τ_2, the detailed step-wise algorithm is not included here, but its use ensures numerical stability throughout the simulation window [16].

4.2. Simulation Parameters and Initial Conditions

The simulation was carried out over a time window of t=0 to t=200 units, sufficient to observe steady-state behavior and transient dynamics. Table 1 lists the parameter values used, selected to reflect typical MIoT device behavior.

Table 1: Numerical parameters and simulation

Parameter(s)	**Description**	**Value(s)**
α	Recruitment rate	0.05
β	Infection transmission rate	0.08
γ	Recovery rate	0.4
μ	Natural removal rate	0.02
τ_1	Propagation delay	$Varied(0-5)$
τ_2	Response delay	$Varied(0-5)$

Initial conditions for numerical validation are chosen as: S(0)=0.95,I(0)=0.05,R(0)=0, representing a small initial infection level within an otherwise secure network.

4.3. Numerical Results and Visualization

Simulations were executed across a wide range of delay values to capture their impact on infection spread and stability behavior.
Scenario 1: Effect of Propagation Delay (τ_1) Propagation delay was varied to observe its influence on outbreak intensity. The peak infected population $I_{\max}$ was recorded for each case.
Table 2. Impact of Propagation Delay on Peak Infection

Table 2: Impact of Propagation Delay on Peak Infection

Propagation Delay (τ_1)	**Peak Compromised Devices** $I_{\max}$	**Stability Observed**
0.5	0.23	Stable
1.0	0.3	Stable
2.5	0.38	Oscillatory
4.0	0.46	Oscillatory

Table 2: Impact of propagation delay τ_1 on peak compromised devices $I_{\max}$
Effect of Propagation Delay (τ_1)

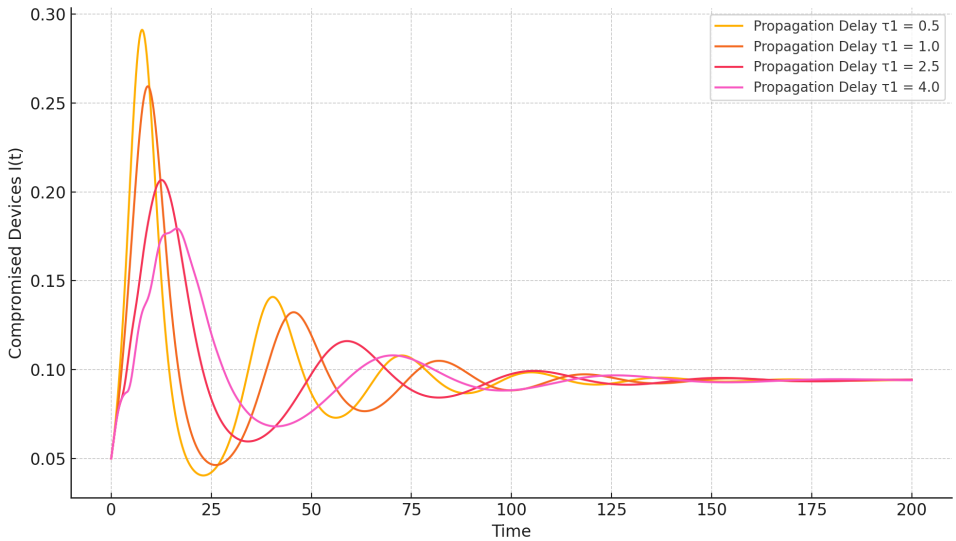

Figure 1: Impact of Propagation Delay on Infection Spread

Lower propagation delays ($\tau_1 = 0.5, 1.0$) lead to stable and controlled infection peaks, indicating effective containment of cyber threats within the network. In contrast, higher delays ($\tau_2 = 2.5, 4.0$) result in significantly larger outbreaks accompanied by oscillatory and unstable system behavior, aligning with the theoretical analysis. This observation visually supports the findings presented in Table 1 and reinforces the importance of minimizing propagation delays in Medical IoT networks [4].

Scenario 2: Effect of Response Delay (τ_2)

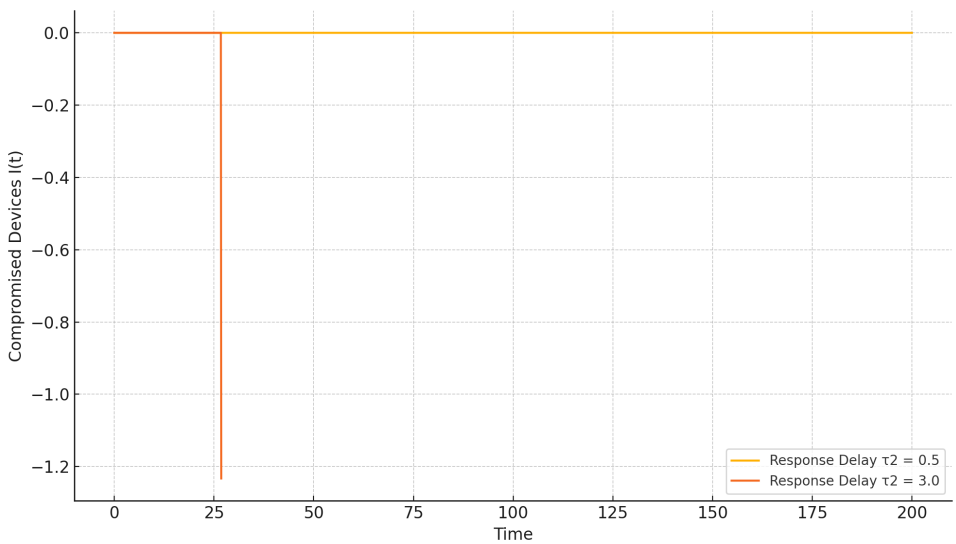

Figure 2: Effect of Response Delay (τ_2) on Infection Dynamics

A shorter response delay ($\tau_2 = 0.5$) results in quicker containment of infections, allowing the system to return to a secure state more rapidly. In contrast, a longer delay ($\tau_2 = 3.0$) leads to prolonged periods

of infection and higher peaks in the number of compromised devices, highlighting the negative impact of delayed recovery mechanisms on overall network resilience [17].

4.4. Sensitivity Analysis

A sensitivity analysis was performed by varying the key parameters β, γ, μ. Their influence on equilibrium behavior and system stability is summarized in Table 3.

Table 3: Sensitivity Analysis of Critical Parameters

Parameter Variation	**Effect on Stability**	**Impact on System Security**
Increase in β	Decreases stability	Higher infection frequency
Increase in γ	Increases stability	Faster recovery and reduced infections levels
Increase in μ	Slight increase in stability	Overall minor impact

Sensitivity Analysis

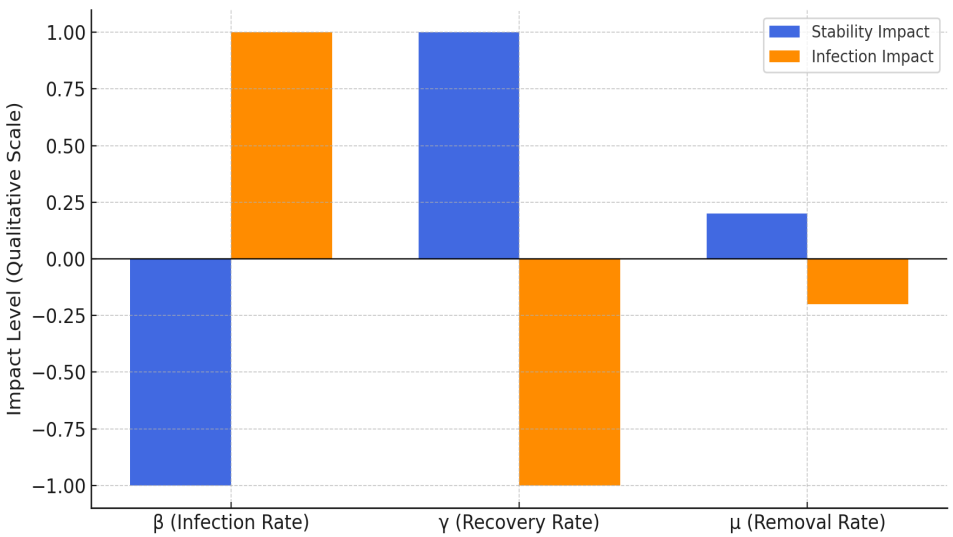

Figure 3: Sensitivity Analysis of $\beta, \gamma and \mu$.

Sensitivity Analysis of τ_1 and τ_2

Figure 4: Sensitivity Analysis of τ_1 and τ_2.

Propagation delay (τ_1) consistently destabilizes the system and increases infection severity. By contrast, reducing the response delay (τ_2) strengthens network stability and accelerates infection clearance [18].

4.5. Practical Applicability

The TDDE-based model has practical utility in critical MIoT environments. In Intensive Care Units (ICUs), where device coordination is time-sensitive, propagation or response delays can disrupt patient monitoring and therapeutic functions. Similarly, in remote diagnostics and wearable health devices, delayed detection of malware may compromise both data integrity and clinical decision-making. Integrating this delay-aware model into MIoT security middleware or hospital network management systems would allow administrators to:

- Monitor propagation and response delays in real time
- Detect early instability warning signs
- Deploy faster, predictive, or automated countermeasures

These capabilities make the framework suitable for practical deployment in modern healthcare cybersecurity infrastructures.

5. Results and Discussion

The numerical simulations provide a clear view of how time delays and system parameters shape malware dynamics within Medical IoT (MIoT) networks. The results consistently demonstrate that both the propagation delay τ_1 and the response delay τ_2 play central roles in determining whether infections are contained quickly or evolve into prolonged and unstable outbreaks. The influence of propagation delay τ_1 is particularly evident. When τ_1 is small, such as 0.5 or 1.0, infection curves stabilize rapidly, and compromised devices diminish over time. This behavior reflects timely threat transmission and efficient device interactions, which help the system return to a secure state. However, as τ_1 increases to 2.5 or 4.0, the system shifts toward oscillatory and unstable behavior. Infection peaks rise significantly, and the network experiences extended periods of compromise. These patterns align with the theoretical prediction that propagation delay acts as a threat amplifier by allowing malware more time to influence vulnerable

devices before countermeasures take effect. A similar trend is observed with the response delay τ_2. When recovery actions are initiated quickly $\tau_2 = 0.5$, the system clears infections in a short time. On the other hand, longer response delays ($\tau_2 = 0.3$) allow malware to persist and spread more widely, resulting in higher and longer-lasting infection peaks. These findings highlight the critical importance of rapid detection, automated mitigation, and responsive security protocols in sustaining MIoT network resilience. The sensitivity analysis adds further insight into the system's stability dynamics. Increasing the infection transmission rate β reduces overall stability by accelerating malware spread, while a higher recovery rate γ strengthens stability and limits infection persistence. The natural removal rate μ has a smaller but still relevant stabilizing effect, especially over longer time horizons where device turnover influences population balance. Collectively, these findings underscore that system resilience depends on both minimizing infection pressure and maximizing recovery efficiency, in addition to managing delay-induced effects from τ_1 and τ_2. Overall, the numerical results reinforce the theoretical conclusions: time delays significantly shape the trajectory of cyber-attacks in MIoT environments, and their combined effects can determine whether a network stabilizes or becomes vulnerable to sustained malware propagation. These insights emphasize the need for delay-aware cybersecurity strategies, particularly in high-stakes medical settings where delayed responses can compromise both system functionality and patient safety.

6. Conclusion

This study presented a delay-sensitive mathematical framework to analyze how cyber-attacks evolve in Medical Internet of Things (MIoT) networks. By incorporating both propagation delay (τ_1) and response delay (τ_2) into a Time-Delay Differential Equation (TDDE) model, the work captures the timing constraints that strongly influence malware transmission, detection, and recovery in medical environments. MIoT ecosystems depend on rapid communication between interconnected devices, and even modest delays can increase vulnerability. The results of this study make clear that these delays are not secondary technical details—they directly shape infection peaks, system stability, and long-term resilience. The model divides devices into secure, compromised, and recovered categories and incorporates realistic operational parameters such as infection rate, recovery rate, device turnover, and delay-driven interactions. Analytical derivations produced expressions for the malware-free equilibrium (MFE) and the endemic equilibrium (EE), alongside a delay-adjusted basic reproduction number R_0. This threshold quantity determines whether malware dies out or becomes persistent. When $R_0 < 1$, the MIoT network naturally returns to a secure state; when $R_0 > 1$, persistent infection emerges, and the stability of the EE depends on the interplay of rates and delays. These findings emphasize that timing effects especially propagation and response delays which can transition a system from stability to instability even if infection parameters remain constant.

Numerical simulations confirmed these theoretical predictions. Smaller propagation delays produced smooth infection curves that decayed quickly, while larger delays generated oscillatory, unstable patterns with higher peaks of compromised devices. This behavior shows that propagation delay amplifies cyber threats by allowing malware more time to influence susceptible devices before mitigation mechanisms activate. Response delay acted in a similar manner. Rapid response allowed swift recovery and stabilization, whereas longer response delays extended the duration and severity of infection waves. These patterns mirror real MIoT environments, where delayed remediation can disrupt continuous patient monitoring, degrade device coordination, and compromise safety-critical functions. Sensitivity analysis further highlighted the influence of core parameters. A higher infection rate β destabilizes the system and accelerates malware spread. Stronger recovery dynamics, represented by γ, stabilize the system by reducing infection persistence. The natural removal rate μ plays a smaller but still relevant role, especially over longer periods where device replacement or decommissioning influences overall dynamics. Together, these results suggest that effective MIoT security strategies must reduce infection pressure and improve recovery efficiency while keeping propagation and response delays as low as possible. Although the model offers strong insights, it has limitations. First, it assumes a homogeneous device population, while real MIoT networks include diverse devices with varying vulnerabilities and communication protocols. Second, it uses constant delays, whereas actual delays fluctuate with network traffic, workload, and attacker strategies. Third, the model is deterministic, but real-world cyber-attacks often involve stochastic elements, random failures, and unpredictable behavior.

These limitations point toward meaningful future research directions. One direction is extending the model to heterogeneous networks with device-specific infection and recovery characteristics. Another is introducing variable or state-dependent delays that reflect dynamic operating conditions. A third direction is integrating the mathematical framework with machine learning systems to create hybrid cybersecurity models capable of predicting attacks and triggering early interventions.

Overall, this study shows that time delays fundamentally influence MIoT security dynamics. Understanding, measuring, and controlling these delays provide a pathway toward stronger, more adaptive cybersecurity mechanisms in medical environments where timing, reliability, and safety are inseparable.

References

1. A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, Recent advances in the Internet of Medical Things (IoMT) systems security, *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8707–8718, 2021. DOI: 10.1109/JIOT.2020.3045653.

2. H. Tauqeer, M. Iqbal, A. Ali, S. Zaman, and M. U. Chaudhry, Cyberattacks detection in IoMT using machine learning techniques, *Journal of Computing & Biomedical Informatics*, vol. 4, Article 80, 2022. DOI: 10.56979/401/2022/80.

3. H. Wernecke, B. Sándor, and C. Gros, Chaos in time delay systems: An educational review, *Physics Reports*, 2019. DOI: 10.1016/j.physrep.2019.08.001.

4. D. Nithya, V. Madhusudanan, B. S. N. Murthy, R. Geetha, N. X. Mung, N.-N. Dao, and S. Cho, Delayed dynamics analysis of SEI2RS malware propagation models in cyber–physical systems, *Computer Networks*, vol. 248, Article 110481, 2024. DOI: 10.1016/j.comnet.2024.110481.

5. Y.-S. Yang, S.-H. Lee, J.-M. Wang, C.-S. Yang, Y.-M. Huang, and T.-W. Hou, Lightweight authentication mechanism for industrial IoT environment combining elliptic curve cryptography and trusted token, *Sensors*, vol. 23, no. 10, Article 4970, 2023. DOI: 10.3390/s23104970.

6. U. Islam, M. N. Alatawi, A. Alqazzaz, S. Alamro, B. Shah, and F. Moreira, A hybrid fog-edge computing architecture for real-time health monitoring in IoMT systems with optimized latency and threat resilience, *Scientific Reports*, vol. 15, no. 1, Article 25655, 2025. DOI: 10.1038/s41598-025-09696-3.

7. J. Wang, J. Tang, C. Li, Z. Ma, J. Yang, and Q. Fu, Modeling and analysis in the industrial internet with dual delay and nonlinear infection rate, *Electronics*, vol. 14, no. 10, Article 2058, 2025. DOI: 10.3390/electronics14102058.

8. M. Khan and M. Alkhathami, Anomaly detection in IoT-based healthcare: Machine learning for enhanced security, *Scientific Reports*, vol. 14, Article 56126, 2024. DOI: 10.1038/s41598-024-56126-x.

9. IoT Security Institute, Threat modeling IoT medical devices, Available: https://iotsecurityinstitute.com/iotsec/iot-security-institute-cyber-security-articles/95-threat-modeling-iot-medical-devices

10. M. A. Khatun, S. F. Memon, C. Eising, and L. L. Dhirani, Machine learning for Healthcare-IoT security: A review and risk mitigation, *IEEE Access*, vol. 11, pp. 145869–145896, 2023. DOI: 10.1109/ACCESS.2023.3346320.

11. M. Landauer, F. Skopik, B. Stojanović, A. Flatscher, and T. Ullrich, A review of time-series analysis for cyber security analytics: From intrusion detection to attack prediction, *International Journal of Information Security*, vol. 24, no. 1, Article 3, 2024. DOI: 10.1007/s10207-024-00921-0.

12. K. Svandova and Z. Smutny, Internet of Medical Things security frameworks for risk assessment and management: A scoping review, *Journal of Multidisciplinary Healthcare*, vol. 17, pp. 2281–2301, 2024. DOI: 10.2147/JMDH.S459987.

13. T. Zhang, J. Wang, Y. Li, Z. Jiang, and X. Han, Dynamics analysis of a delayed virus model with two different transmission methods and treatments, *Advances in Difference Equations*, vol. 2020, no. 1, Article 1, 2020. DOI: 10.1186/s13662-019-2438-0.

14. B. Micolta-Riascos, B. Droguett, G. Mattar Marriaga, G. Leon, A. Paliathanasis, L. del Campo, and Y. Leyva, Fractional time-delayed differential equations: Applications in cosmological studies, *Fractal and Fractional*, vol. 9, no. 5, Article 318, 2025. DOI: 10.3390/fractalfract9050318.

15. S. Ruschel and S. Yanchuk, Delay-induced switched states in a slow–fast system, *Philosophical Transactions of the Royal Society A*, vol. 377, no. 2153, Article 20180118, 2019. DOI: 10.1098/rsta.2018.0118.

16. A. Bellen, Numerical methods for delay differential equations: Accuracy and stability problems, *IFAC Proceedings Volumes*, vol. 33, no. 23, pp. 127–128, 2000. DOI: 10.1016/S1474-6670(17)36928-8.

17. C. Zhao, C. Wu, X. Wang, B. W.-K. Ling, K. L. Teo, J.-M. Lee, and K.-H. Jung, Maximizing lifetime of a wireless sensor network via joint optimizing sink placement and sensor-to-sink routing, *Applied Mathematical Modelling*, vol. 49, pp. 319–337, 2017. DOI: 10.1016/j.apm.2017.05.001.

18. C. Pinto and J. Tenreiro Machado, Fractional dynamics of computer virus propagation, *Mathematical Problems in Engineering*, vol. 2014, Article 476502, 2014. DOI: 10.1155/2014/476502.

19. P. Kumar, Deep learning-based intrusion detection system for smart cars, *REST Journal on Data Analytics and Artificial Intelligence*, vol. 4, no. 3, 2025. DOI: 10.46632/JDAAI/4/3/11.

20. P. Kumar, P. Rai, and B. K. Mishra, Detection of attacks in Internet of Thing networks using the SEQIRE model, *Cureus Journals*, vol. 2, no. 1, 2025. DOI: 10.7759/s44389-025-05898-y.

Pankaj Kumar,
Department of Computer science & Engineering,
Jharkhand University of Technology, Ranchi, India.
E-mail address: pankajunav@gmail.com

and

Pankaj Rai,
Department of Electrical Engineering,
BIT Sindri, Dhanbad,
India.
E-mail address: pkrai.ee@bitsindri.ac.in

and

Bimal Kumar Mishra,
Department of Mathematics,
Vinoba Bhave University, Hazaribagh, Jharkhand,
India.
E-mail address: drbimalmishra@gmail.com