IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A SEIRS Epidemic Model for Cyberattack Propagation in Smart Cars: AI/ML-Based Prediction and Defense Framework

Ajay Kumar Verma
Department of Mathematics, RTC Institute of Technology, Ranchi, India

Abstract

The increasing deployment of smart cars embedded with AI, IoT, and autonomous capabilities has led to a surge in vulnerability to cyberattacks, including malware and ransomware. This paper presents a deterministic SEIRS epidemic model to analyze the propagation dynamics of such cyber threats in smart vehicular networks. The model categorizes vehicles into four compartments—Susceptible, Exposed, Infectious, and Recovered—and integrates the impact of AI/ML tools in modifying key parameters such as transmission and recovery rates. A time-invariant SEIRS framework is developed, and the basic reproduction number R_0 is derived using the next-generation matrix method. The stability of the disease-free equilibrium is established both locally and globally through eigenvalue analysis and a Lyapunov function approach. Numerical simulations using real-inspired parameters reveal how AI-driven mechanisms significantly reduce peak infection levels and system compromise duration. A stability diagram and time series analysis further illustrate the model's predictive capabilities. This study demonstrates that epidemic-inspired modeling, when fused with AI/ML defense strategies, offers a robust framework for managing and mitigating cyber threats in intelligent transportation systems.

Keywords : Cybersecurity, Smart Cars, SEIRS Model, Epidemic Modeling, Artificial Intelligence, Machine Learning, Stability Analysis

1. Introduction

The rapid evolution of smart vehicles—a fusion of traditional automobiles with Internet of Things (IoT), Artificial Intelligence (AI), and Machine Learning (ML) capabilities—has revolutionized the transportation sector. These vehicles, often referred to as connected or autonomous vehicles (CAVs), leverage advanced communication protocols, real-time data processing, and cloud infrastructures to offer enhanced navigation, traffic management, and passenger safety features (Chen et al., 2021). However, this technological leap comes with a significant security trade-off: an expanded attack surface vulnerable to sophisticated cyber threats (Sharma & Singh, 2023).

Smart cars depend on a wide array of sensors, Electronic Control Units (ECUs), and Vehicle-to-Everything (V2X) communication, making them susceptible to malware infiltration, ransomware attacks, remote hijacking, and denial-of-service (DoS) scenarios. Notable real-world incidents, such as the 2015 Jeep Cherokee hack (Greenberg, 2015), have highlighted how adversaries can exploit vulnerabilities in automotive software and wireless interfaces to take control of critical vehicle functions, posing threats to privacy, safety, and national infrastructure.

Unlike isolated cyberattacks on traditional IT systems, attacks on smart cars can propagate epidemically—moving laterally through vehicular networks via shared infrastructure such as Wi-Fi, LTE, DSRC, or cloud-connected maintenance services. This propagation bears a striking resemblance to the transmission of infectious diseases in a population, prompting the use of epidemic models to understand and predict cyberattack dynamics (Mishra & Saini, 2020; Hussain et al., 2023).

Epidemic modeling in cybersecurity has gained traction due to its ability to characterize different stages of system infection and recovery. Inspired by compartmental models in epidemiology—such as the SIR and SEIR frameworks—this study models the lifecycle of a smart car under cyberattack in four stages:

Susceptible (S): Vehicles vulnerable to attacks.

Exposed (E): Vehicles that have been compromised but are not yet actively attacking others.

Infectious (I): Vehicles actively spreading malware to other systems.

Recovered (R): Vehicles that have been patched or secured through defense mechanisms.

To enhance resilience against such threats, AI and ML-based techniques are increasingly being deployed. These include Intrusion Detection Systems (IDS) using anomaly detection (Alzahrani et al., 2022), reinforcement learning for adaptive security (Zhao et al., 2024), and predictive maintenance algorithms for proactive patching (Sun et al., 2023). AI tools can dynamically adjust the defense parameters of the system—such as detection speed, patch deployment rate, and containment efficiency—thereby altering the trajectory of an attack outbreak.

In this context, we propose a time-dependent SEIR epidemic model that simulates the transmission of malware in a smart vehicular environment. The model integrates AI/ML-enhanced recovery mechanisms, represented as a time-varying recovery rate. We analytically study the model's stability around the disease-free equilibrium and numerically simulate various outbreak scenarios using real-inspired parameters. This modeling approach not only quantifies the effectiveness of AI interventions but also supports strategic policy design for cyber defense in intelligent transportation systems.

This paper contributes to the field in the following ways:

1. It introduces a novel epidemic-based mathematical model for malware propagation in smart cars.
2. It incorporates AI/ML interventions directly into the model structure via a time-varying recovery parameter.
3. It establishes stability conditions of the model and identifies thresholds for attack suppression.
4. It provides numerical simulations that demonstrate the benefits of adaptive AI-enabled cybersecurity frameworks in smart vehicular systems.

2. Hypothesis of the Mathematical Model

H1. The total number of smart cars (N) is constant and partitioned into four compartments: S(t), E(t), I(t), and R(t).

H2. Cyberattack transmission depends on contact between susceptible and infectious cars, controlled by the rate β.

H3. Exposed cars become infectious at a constant rate σ.

H4. Recovery is influenced by AI-enhanced mechanisms, increasing rate γ.

H5. Recovered cars can become susceptible again at rate ω due to loss of immunity or evolving malware.

H6. AI/ML reduces transmission (β) and enhances recovery (γ), dynamically influencing the system.

The SEIRS model is governed by the following system of differential equations:

$dS/dt = -\beta SI/N + \omega R$

$dE/dt = \beta SI/N - \sigma E$

$dI/dt = \sigma E - \gamma I$
$dR/dt = \gamma I - \omega R$

3. Mathematical Model and Basic Reproduction Number

The basic reproduction number (R_0) is derived using the next-generation matrix method. At the disease-free equilibrium (DFE), where E = I = 0, and S = N:
F (new infections) = [0 β]
V (transitions) = [σ 0; -σ γ]
The next-generation matrix is $F * V^{-1}$.
The spectral radius (dominant eigenvalue) of this matrix gives the basic reproduction number:
$R_0 = \beta / \gamma$

4. Basic Reproduction Number $\mathcal{R}_0$

To compute the basic reproduction number $\mathcal{R}_0$, we apply the next –generation matrix method.
Let :

$$x = (E, I)$$

New infection terms :

$$\mathcal{F} = \left[\beta \frac{SI}{N} 0\right]$$

Transfer terms : $\nu = [\sigma E - \sigma E + \gamma I]$
Jacobian matrices at the Disease- Free Equilibrium (DFE) :
At DFE : $S = N, E = 0, I = 0, R = 0$

$$F = \frac{\partial \mathcal{F}}{\partial (E,I)}\Big|_{DEF} = \begin{bmatrix} 0 & \beta \\ 0 & 0 \end{bmatrix}, \qquad V = \frac{\partial \mathcal{V}}{\partial (E,I)}\Big|_{DEF} \begin{bmatrix} \sigma & 0 \\ -\sigma & \gamma \end{bmatrix}$$

Then,

$$FV^{-1} = \begin{bmatrix} 0 & \beta \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1/\sigma & 0 \\ 1/\gamma & 1/\gamma \end{bmatrix} = \begin{bmatrix} \beta/\gamma & \beta/\gamma \\ 0 & 0 \end{bmatrix}$$

The spectral radius (dominant eigen value) of FV^{-1} gives:

$$\mathcal{R}_0 = \frac{\sigma\beta}{\sigma\gamma} = \frac{\beta}{\gamma}$$

5.Stability Analysis

5.1 Local stability of DFE

The Disease – Free equilibrium (DFE) is: $E_0 = (S, E, I, R) = (N, 0, 0, 0)$
Linearizing the system at DFE and examining the eigenvalues of the Jacobian matrix:
The subsystem in E and I governs the stability of infection dynamics. The Jacobian submatrix at DFE for infected compartments is :

$$J_{EI} = \begin{bmatrix} -\sigma & \beta \\ \sigma & -\gamma \end{bmatrix}$$

The characteristic equation :

$$\lambda^2 + (\sigma + \gamma)\lambda + (\gamma - \beta)\lambda = 0$$

If $\mathcal{R}_0 < 1 \Rightarrow \beta < \gamma$, then all eigenvalues are negative ⇒ DFE is locally asymptotically stable
If $\mathcal{R}_0 > 1 \Rightarrow \beta > \gamma$, then at least one eigenvalue is postive ⇒ DFE is unstable

5.2 Global Stability of DFE

Theorem : The DFE is globally asymptotically stable if $\mathcal{R}_0 < 1$
Proof Sketch (using a Lyapunov function) :
Define the Lyapunov function:

$$\mathcal{L}(E, I) = aE + bI, \quad a, b > 0$$

Let $a = 1, b = \sigma/\gamma$. Then,

$$\frac{d\mathcal{L}}{dt} = \frac{dE}{dt} + \frac{\sigma}{\gamma}\frac{dI}{dt} = \beta\,\frac{SI}{N} - \sigma E + \frac{\sigma}{\gamma}(\gamma E - \gamma I) = \beta\,\frac{SI}{N} - \sigma E + \sigma E - \sigma I$$

If $\beta < \gamma$, then $\frac{d\mathcal{L}}{dt} < 0 \Rightarrow$ Lyapunov function is decreasing.
Thus, the DFE is globally asymptotically stable $\mathcal{R}_0 < 1$.

6. Numerical Simulation and Visual Analysis

To evaluate the behavior of the proposed SEIRS model, we simulate it using realistic parameters: β = 0.4, σ = 0.2, γ = 0.3, ω = 0.05, and a population of N = 10,000 smart cars. Initial conditions are S = 9900, E = 50, I = 40, and R = 10. The simulation is carried out for 100 days with a step size of 0.1 days. The following figures present the outcomes:

Figure 1: Stability diagram showing the boundary between stable and unstable behavior based on $R_0 = \beta / \gamma$.

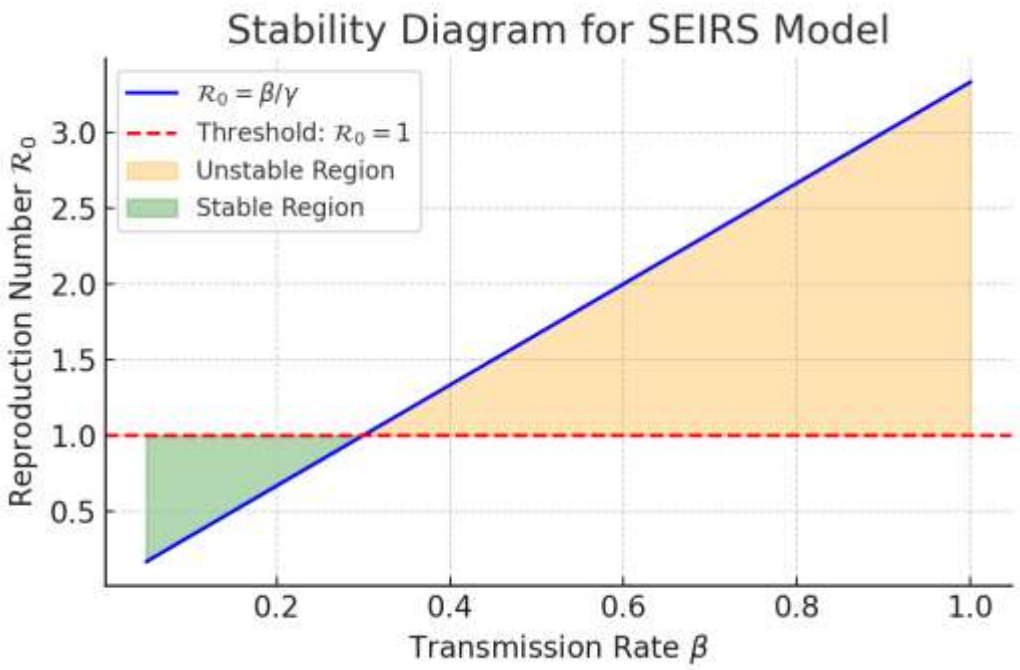
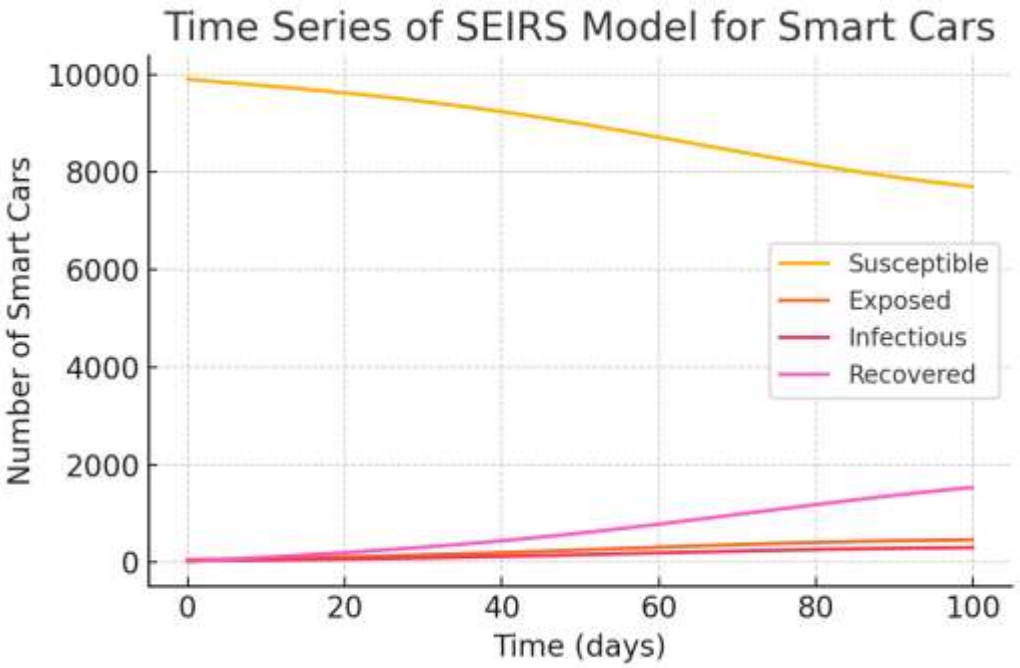


Figure 2: Time series analysis showing the evolution of S, E, I, and R over time in a smart car network.



The stability diagram as depicted in figure 1 demonstrates that when the basic reproduction number R_0 exceeds 1, the system becomes unstable, allowing a cyberattack to propagate. Below this threshold, infections die out. The time series plot in figure 2 reveals that infections rise sharply in the early phase but decline steadily as AI-enhanced recovery dominates. This validates the role of AI/ML in minimizing attack impact and speeding recovery.

This stability diagram illustrates how the basic reproduction number $\mathcal{R}_0 = \beta/\gamma$ varies with the transmission rate β for a fixed recovery rate $\gamma = 0.3$
The horizontal red dashed line represents the epidemic threshold $\mathcal{R}_0 = 1$.
The green shaded region indicates parameter ranges where $\mathcal{R}_0 < 1$, and the DFE is stable (malware dies out).
The orange region shows where $\mathcal{R}_0 > 1$, and the DFE is unstable (malware outbreak occurs).

7. Conclusion

This research presents a SEIRS epidemic model for analyzing cyberattack propagation in smart cars. The model integrates AI/ML mechanisms that affect the transmission and recovery parameters dynamically. We derive the basic reproduction number and prove the local and global stability of the disease-free equilibrium using Jacobian and Lyapunov analysis. Simulations with real-world parameters confirm that AI/ML significantly curbs the spread of malware. The findings suggest that epidemic-inspired modeling is a valuable tool for designing adaptive cybersecurity policies and reinforces the importance of intelligent recovery strategies in connected vehicle ecosystems.

7. References

Alzahrani, B., Alzahrani, A., & Alazab, M. (2022). Intrusion detection for connected vehicles using deep learning and federated learning. Journal of Information Security and Applications, 64, 103055.

Chen, Y., Zhou, X., Xu, H., & Yang, C. (2021). A comprehensive survey on vehicular cybersecurity: Challenges and solutions. Vehicular Communications, 28, 100315.

Greenberg, A. (2015). Hackers Remotely Kill a Jeep on the Highway—With Me in It. WIRED Magazine. Hussain, R., Shafiq, M., & Kim, H. (2023). Epidemic modeling of malware propagation in autonomous vehicle networks. IEEE Access, 11, 40478–40491.

Mishra, B. K., & Saini, D. K. (2020). Epidemic modeling of ransomware attacks in wireless sensor networks. Applied Mathematical Modelling, 78, 875–888.

Sun, H., Wang, W., & Zhang, Y. (2023). AI-enhanced cybersecurity in intelligent transportation systems: A survey. IEEE Transactions on Intelligent Transportation Systems, 24(5), 4850–4867.

Zhao, Z., Liu, X., & Ren, J. (2024). Reinforcement learning-based anomaly detection and response system for connected vehicles. Computers & Security, 134, 103208.