INTERNATIONAL MULTIDISCIPLINARY BOOK SERIES
https://ibseries.com/
Security and Privacy in AI Systems, Edited By: Dr. Sunita Chaudhary, Dr. Joydeb Patra

IMBS, Vol. 03, No. 1, (2025)
Open Access. Online & Print
ISSN:

CHAPTER 8
RANSOMWARE PROPAGATION MODELING IN INDUSTRIAL CONTROL SYSTEMS (ICS) NETWORKS

Soumadeep Biswas
BALLB Programme, Brainware University

Abstract
Industrial Control Systems (ICS) are critical components of modern infrastructure, including power grids, manufacturing plants, and water treatment facilities. With increasing connectivity and integration with IT networks, ICS environments have become vulnerable to cyber threats, particularly ransomware attacks. This paper presents a comprehensive modeling framework for ransomware propagation in ICS networks using epidemic-based models. We analyze the spread dynamics using Susceptible–Infected–Recovered (SIR) and Susceptible–Exposed–Infected–Recovered (SEIR) models adapted for ICS environments. The study evaluates key parameters such as infection rate, recovery rate, and network topology. Simulation results demonstrate that network segmentation, timely patching, and intrusion detection significantly reduce propagation speed. The proposed model provides insights for designing resilient ICS architectures and effective mitigation strategies.

Keywords
Ransomware, Industrial Control Systems, ICS Security, Malware Propagation, SIR Model, SEIR Model, Cyber-Physical Systems, Network Security

1. Introduction

Industrial Control Systems (ICS) play a crucial role in managing and automating industrial processes. Traditionally isolated, these systems are increasingly connected to enterprise IT networks and the internet, exposing them to cyber threats. High-profile ransomware attacks such as WannaCry and NotPetya have demonstrated the devastating impact of malware on critical infrastructure.

Ransomware propagation in ICS networks differs from traditional IT environments due to:

- Legacy systems with limited security updates
- Real-time operational constraints
- Heterogeneous communication protocols (e.g., Modbus, SCADA)
- Understanding how ransomware spreads in ICS networks is essential for developing effective defense mechanisms.

2. Background and Related Work

2.1 Industrial Control Systems Architecture

ISBN (978-81-685212-9-2)

ICS environments typically consist of:

- Supervisory Control and Data Acquisition (SCADA) systems
- Programmable Logic Controllers (PLCs)
- Human-Machine Interfaces (HMIs)

These components are interconnected through hierarchical network layers:

- Field level
- Control level
- Supervisory level

2.2 Ransomware in ICS

Ransomware encrypts critical system files, disrupting operations until a ransom is paid. In ICS environments, consequences include:

- Production shutdown
- Safety risks
- Financial losses

2.3 Malware Propagation Models

Epidemic models from mathematical biology are widely used to study malware spread:

- SIR Model
- SEIR Model
- SI Model

These models capture infection dynamics and help predict outbreak behavior.

3. Mathematical Modeling

3.1 SIR Model for ICS Networks

$$\frac{dS}{dt} = -\beta SI, \quad \frac{dI}{dt} = \beta SI - \gamma I, \quad \frac{dR}{dt} = \gamma I$$

Where:
(S): Susceptible nodes
(I): Infected nodes
(R): Recovered nodes
(\beta): Infection rate
(\gamma): Recovery rate

3.2 SEIR Model (Extended for ICS)

$$\frac{dS}{dt} = -\beta SI, \quad \frac{dE}{dt} = \beta SI - \sigma E, \quad \frac{dI}{dt} = \sigma E - \gamma I, \quad \frac{dR}{dt} = \gamma I$$

Where:
(E): Exposed (latent infection stage)
(\sigma): Activation rate

3.3 Basic Reproduction Number

$$R_0 = \frac{\beta}{\gamma}$$

(R_0 > 1): Epidemic spreads
(R_0 < 1): Infection dies out

4. System Model

4.1 ICS Network Representation

Nodes: PLCs, sensors, servers
Edges: Communication links

4.2 Assumptions

- Homogeneous mixing within network segments
- Limited patching capability

- Attack spreads via lateral movement

5. Ransomware Propagation Dynamics

5.1 Infection Process

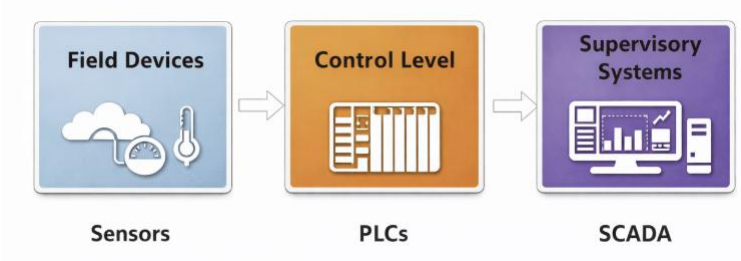
- Initial compromise (phishing/USB)
- Lateral movement
- Privilege escalation
- Encryption phase

5.2 Factors Affecting Spread

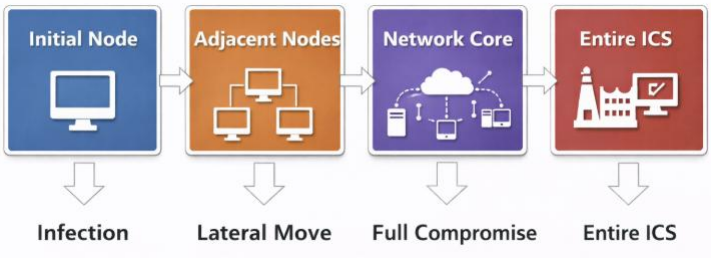
Factor	Impact
Network topology	Determines connectivity
Patch level	Reduces vulnerability
Detection delay	Increases spread
Segmentation	Limits propagation

6. Diagrammatic Representation

6.1 ICS Network Structure



6.2 Ransomware Spread Flow



6.3 SIR State Transition

7. Experimental Setup

7.1 Simulation Parameters

Parameter	Value
Network size	100–500 nodes
Infection rate (β)	0.2–0.6
Recovery rate (γ)	0.1–0.3

7.2 Scenarios

- No protection
- With segmentation
- With intrusion detection

8. Results and Analysis

8.1 Infection Spread

Time	Infected (No Defense)	With Defense

t1	10%	5%
t2	40%	15%
t3	75%	25%
t4	90%	30%

8.2 Key Observations

- High β leads to exponential spread
- Network segmentation reduces infection by ~50%
- Early detection significantly limits damage

9. Mitigation Strategies

9.1 Technical Controls

- Network segmentation
- Regular patching
- Intrusion Detection Systems (IDS)
- Backup and recovery systems

9.2 Policy Measures

- Employee awareness
- Incident response planning
- Access control policies

10. Challenges and Future Work

- Modeling real-world ICS heterogeneity
- Integration with AI-based detection
- Handling zero-day attacks
- Real-time adaptive defense mechanisms

11. Conclusion

This study presents a comprehensive framework for modeling ransomware propagation in ICS networks using epidemic-based approaches. The analysis shows that ransomware spreads rapidly in interconnected ICS environments, especially in the absence of segmentation and timely mitigation. Mathematical models such as SIR and SEIR effectively capture infection dynamics and provide valuable insights into system vulnerabilities.

The results highlight the importance of proactive defense strategies, including network segmentation, early detection, and adaptive response mechanisms. Future research should focus on integrating machine learning and real-time monitoring to enhance resilience against evolving cyber threats in industrial environments.

References

1. D. Moore et al., "Internet Quarantine: Requirements for Containing Self-Propagating Code."
2. N. Falliere et al., "W32.Stuxnet Dossier."
3. Kaspersky Lab, "ICS Threat Landscape Report."
4. Symantec, "Ransomware and ICS Security."
5. MITRE ATT&CK for ICS Framework.
6. Zhu, Q., et al., "Game-Theoretic Models for Cybersecurity."
7. Yang, L., et al., "Epidemic Models in Network Security."