Attack-Defense Game-Driven Virus Propagation Model for Wireless Sensor Networks: Postprint

Authors: Zhou Haiping, Shen Shigen, Huang Longjun, Liu Ni

Date: 2019-01-03T00:00:00+00:00

Abstract

Traditional wireless sensor network (WSN) virus propagation models directly specify infection probability and recovery probability without analyzing the rationale behind their values. From a game-theoretic perspective, we analyze the microscopic mechanism of virus propagation in WSN, establish an attack-defense game model for WSN, derive the mixed Nash equilibrium solution of the game model, and determine node infection probability and cure probability according to the mixed Nash equilibrium strategies of both players, thereby establishing a virus propagation model for WSN. Furthermore, we employ the cellular automaton method to simulate the virus propagation process in WSN. Theoretical analysis and computer simulations reveal the relationship between virus propagation outcomes and game parameters, and the research results offer certain guidance for formulating measures to suppress virus propagation.

Full Text

Preamble

Virus Propagation Model for Wireless Sensor Networks Driven by Attack-Defense Game

Zhou Haiping[1], Shen Shigen[1], Huang Longjun[1], Liu Ni[2]
(1. Department of Computer Science & Engineering, Shaoxing University, Shaoxing, Zhejiang 312000, China;
2. Department of Mathematics & Information Science, Guiyang College, Guiyang 550005, China)

Abstract: Traditional virus propagation models for Wireless Sensor Networks (WSN) directly specify infection and recovery probabilities without analyzing the underlying rationale for their values. This paper analyzes the microscopic

mechanism of virus propagation in WSN from a game-theoretic perspective, establishes an attack-defense game model for WSN, derives the mixed Nash equilibrium solution of the game model, and determines the infection probability and cure probability for nodes based on the mixed Nash equilibrium strategies of both parties, thereby constructing a virus propagation model for WSN. Furthermore, the paper simulates the virus propagation process using cellular automata methods. Theoretical analysis and computer simulation reveal the relationship between virus propagation outcomes and game parameters. The research findings provide guidance for developing measures to suppress virus propagation.

Keywords: wireless sensor networks; virus propagation; attack-defense game; cellular automaton

0 Introduction

With the development of Internet of Things technology, Wireless Sensor Networks (WSN) have been successfully applied in numerous fields including transportation, environmental monitoring, and military reconnaissance [1,2]. However, due to the limited storage and computational capabilities of wireless sensor nodes, they are vulnerable to malicious program attacks [3,4]. Common attack methods include channel interference, identity spoofing, and virus propagation [5,6]. Among these, malicious virus propagation represents a particularly severe threat because once a node is infected, it can further propagate the virus to other nodes, leading to rapid network collapse [7,8].

To date, extensive research has been conducted separately on WSN attack-defense detection and malicious program propagation. In the area of WSN attack-defense research, Zhang Kejing et al. analyzed attack and defense strategies between malicious nodes and defense systems from a game-theoretic perspective, then used evolutionary dynamics methods to obtain the game equilibrium solution, providing guidance for WSN defense processes [9]. Liu Yi et al. proposed an evolutionary game-based attack-defense model for energy consumption attacks in industrial WSN, obtained the evolutionary stable strategies for both parties, and provided feasible strategies for defending against energy consumption attacks [10]. Reference [11] used data mining technology for feature recognition of DoS attacks and employed feature selection algorithms to further refine key features, reducing time complexity while improving DoS attack recognition rates.

In virus propagation research, Zheng Rongjun et al. studied the propagation behavior of multiple worm viruses in WSN using infectious disease dynamics theory [12], obtaining network propagation characteristics when multiple viruses interact. Reference [13] applied traditional infectious disease propagation theory to the malicious program propagation process in WSN, treating malicious programs and intrusion detection systems (IDS) as two opposing agents and establishing

a differential game model between them. Through analysis and solution of the game model, they obtained equilibrium strategies that could suppress malicious program propagation while reducing detection costs. Reference [14] proposed a virus propagation model incorporating individual differences, where different nodes have different attack resistance capabilities, and research results showed that heterogeneity in node resistance significantly affects virus propagation effectiveness. Reference [15] studied virus propagation when mobile agents in WSN are attacked, finding that viruses spread more easily when mobile agents are compromised.

In existing research on WSN malicious program propagation, infection and cure probabilities are typically specified directly when establishing propagation models, without considering the underlying microscopic mechanisms. However, in real WSNs, infection and cure probabilities are determined by the strategies adopted by attackers and defenders. For this reason, this paper analyzes the strategies of both parties from a game-theoretic perspective and determines infection and cure probabilities based on these strategies, thereby revealing how game parameters affect propagation efficiency. The paper is organized as follows: (a) establish the attack-defense game model in WSN and derive the Nash equilibrium strategy; (b) based on the game strategies of both parties, establish the SIS virus propagation model for WSN and obtain the relationship between virus propagation speed and game parameters through model solution; (c) conduct numerical simulation and verification of the theoretical model, and compare and analyze the simulation results with analytical results from the theoretical model.

---

1 Attack-Defense Game Model for WSN

WSN contains both malicious nodes and legitimate nodes. Malicious nodes are those infected with viruses that propagate to legitimate nodes, while legitimate nodes use IDS to detect received information. Legitimate nodes consume energy when using IDS to detect information. Due to limited node energy, legitimate nodes cannot detect all received information without quickly depleting their energy and ceasing to function. To extend their lifespan, legitimate nodes detect received information with a certain probability. For malicious nodes, frequent attacks quickly expose their identity, so malicious nodes also attack with a certain probability. Thus, the attack-defense process between legitimate and malicious nodes is essentially a game, which this paper analyzes using game theory.

Definition 1. The attack-defense game model in WSN can be represented as a three-tuple $\langle N, S, u \rangle$, where:
a) $N = \{\text{legitimate node}, \text{malicious node}\}$ represents the set of participants;
b) $S_{\text{legitimate node}} = \{\text{detect}, \text{not detect}\}$, $S_{\text{malicious node}} = \{\text{attack}, \text{not attack}\}$ represent the strategy sets. Note that the "not attack" strategy for malicious

nodes means sending normal information rather than sending no information; c) u_i represents the payoff obtained by participant i during the game, with values determined by the strategies adopted by both parties.

Table 1 provides definitions of symbols used in this paper, and Table 2 presents the payoff matrix for both parties.

Table 1 Symbolic Definition

Symbol	Definition
a	Payoff for legitimate node when detecting virus; loss for malicious node when identified
b	Payoff for malicious node when attack succeeds; loss for legitimate node when infected
e_S	Energy cost for legitimate node to detect received information
e_I	Energy cost for malicious node to send virus or normal information
x	Probability of malicious node launching attack
y	Probability of legitimate node conducting detection
E_U	Expected payoff for legitimate node in attack-defense game
E_I	Expected payoff for malicious node in attack-defense game

Table 2 Game Payoff for Legitimate Node and Malicious Node

	Legitimate Node: Detect	Legitimate Node: Not Detect
Malicious Node: Attack	$(-e_S - e_I, a - e_I)$	$(-b, b - e_I)$
Malicious Node: Not Attack	$(-e_S, -e_I)$	$(0, -e_I)$

For the game to be meaningful, the model must satisfy $a > e_S$ and $b > e_I$. Under these conditions, when malicious nodes attack, the best strategy for legitimate nodes is to detect; otherwise, not to detect. For malicious nodes, when legitimate nodes detect, the best strategy is not to attack; otherwise, to attack. Since neither party knows the other' s action, this game model has no pure strategy Nash equilibrium. The following analysis examines both parties' attack-defense behaviors from the perspective of mixed equilibrium strategies.

Theorem 1. The attack-defense game model in WSN has a mixed Nash equilibrium strategy $\langle x^*, y^* \rangle$, where $x^* = \frac{e_S}{a+e_S}$ and $y^* = \frac{e_I}{b+e_I}$.

Proof. Assume malicious nodes attack with probability x and do not attack with probability $1-x$, while legitimate nodes detect with probability y and do not detect with probability $1-y$. Based on the payoff matrix, the expected payoff for legitimate nodes E_U is:

$$E_U = y[x(-e_S - e_I) + (1-x)(-e_S)] + (1-y)[x(-b) + (1-x)(0)]$$

Simplifying:

$$E_U = -xy(a+e_S) - e_S(1-x) - xb(1-y)$$

Taking the partial derivative with respect to y and setting it to zero:

$$\frac{\partial E_U}{\partial y} = -x(a+e_S) + xb = 0$$

Solving yields:

$$x^* = \frac{e_S}{a+e_S}$$

Similarly, the expected payoff for malicious nodes E_I is:

$$E_I = x[y(a-e_I) + (1-y)(b-e_I)] + (1-x)[y(-e_I) + (1-y)(-e_I)]$$

Simplifying:

$$E_I = xy(a-b) + x(b-e_I) - e_I$$

Taking the partial derivative with respect to x and setting it to zero:

$$\frac{\partial E_I}{\partial x} = y(a-b) + (b-e_I) = 0$$

Solving yields:

$$y^* = \frac{e_I}{b+e_I}$$

Thus, $\langle x^*, y^* \rangle$ constitutes the mixed Nash equilibrium strategy for the attack-defense game between malicious and legitimate nodes.

---

2 Game-Driven Virus Propagation Model for WSN

From the game model, rational malicious and legitimate nodes will attack and detect with probabilities x^* and y^*, respectively. When a malicious node attacks and a legitimate node fails to detect, the legitimate node becomes infected. When a malicious node attacks while the legitimate node enables detection, the malicious node is identified, cleared of the virus, and restored as a legitimate node. Therefore, the infection probability for legitimate nodes is $x^*(1-y^*)$, while the cure probability for malicious nodes is x^*y^*.

Assume malicious nodes constitute proportion i of total network nodes and legitimate nodes constitute proportion s. The virus propagation evolution model in WSN can be described by the equation system:

$$\begin{cases} \frac{di}{dt} = x^*(1-y^*)si - x^*y^*i \\ \frac{ds}{dt} = -x^*(1-y^*)si + x^*y^*i \\ i+s=1 \end{cases} \tag{7}$$

Substituting $x^* = \frac{e_S}{a+e_S}$ and $y^* = \frac{e_I}{b+e_I}$ into equation (7) and simplifying yields:

$$\frac{di}{dt} = \frac{ab - e_S e_I}{(a+e_S)(b+e_I)} i(1-i) \tag{9}$$

Let $c = \frac{ab-e_S e_I}{(a+e_S)(b+e_I)}$, and assume the initial infection proportion is i_0 at $t=0$. Integrating equation (9) from 0 to t gives:

$$\ln \frac{i}{i_0} - \ln \frac{1-i}{1-i_0} = ct \tag{10}$$

Further solving equation (10) yields:

$$i(t) = \frac{i_0 e^{ct}}{1 - i_0 + i_0 e^{ct}} \tag{12}$$

Equation (12) shows that virus propagation is ultimately determined by the payoff parameters of the game model. Numerical simulation of equation (12) reveals the relationship between game parameters and network node infection proportion, as shown in Figures 1 [Figure 1: see original paper] through 3 [Figure 3: see original paper]. When $a > b$ (Figure 1), the network node infection proportion reaches 1 over time, meaning all nodes eventually become infected, and virus propagation speed increases with detection energy cost e_S. When $a = b$ (Figure 2 [Figure 2: see original paper]), the infection proportion remains constant at the initial value, unaffected by changes in detection energy cost e_S. When $a < b$ (Figure 3 [Figure 3: see original paper]), the network node infection proportion reaches 0 over time, meaning the virus disappears completely from the network, and propagation speed decreases with increasing detection energy cost e_S.

3 Cellular Automata Simulation

While the theoretical model adequately describes malicious program propagation in WSN, it has limitations. Real sensor nodes have limited communication ranges and can only communicate with nearby nodes, which the theoretical model does not consider. Additionally, some sensor networks have mobile nodes, making the network dynamic—a scenario existing theoretical models cannot handle. To make research results more realistic, this section simulates WSN virus propagation using cellular automata methods.

3.1 Simulation Steps

a) Generate a 100×100 grid as shown in Figure 4 [Figure 4: see original paper], randomly deploying sensor nodes in proportion p_w.

b) Establish connections between any two sensor nodes if their distance does not exceed r, thereby determining the sensor network structure.

c) At the initial moment, randomly set proportion i_0 of nodes as malicious nodes.

d) Each malicious node randomly selects a directly connected node to send information, with probability x^* of sending malicious information and probability $1 - x^*$ of sending normal information.

e) When a malicious node sends information to another malicious node, the information is discarded. When sending to a legitimate node, the legitimate node detects with probability y^*. If a legitimate node receives a virus and happens not to detect, it becomes infected. If a legitimate node detects the received virus, the malicious node is identified, repaired, and converted back to a legitimate node.

f) If t is less than the preset simulation steps, increment t by 1 and return to step d); otherwise, terminate.

3.2 Simulation Results

Setting parameters $p_w = 0.1$ and $i_0 = 0.05$, the above simulation steps were executed to examine the impact of game parameters on virus propagation outcomes. Simulation results are shown in Figures 5 [Figure 5: see original paper] through 7 [Figure 7: see original paper]. The figures demonstrate that when $a > b$, the proportion of malicious nodes in the network increases over time until all nodes are infected, and virus propagation speed increases with detection energy cost e_S. When $a = b$, the proportion of malicious nodes fluctuates around the initial infection proportion over time. When $a < b$, the proportion of malicious nodes decreases over time until all nodes become legitimate. These conclusions are consistent with the theoretical results from the previous section.

Additionally, since virus propagation in WSN is related to communication radius, this paper further investigated the impact of sensor node communication radius on virus propagation speed. By varying the communication radius, propagation curves under different radii were obtained. Figure 8 [Figure 8: see original paper] shows that with other parameters fixed, virus propagation speed increases with communication radius.

---

4 Discussion

4.1 Comparison of Theoretical and Simulation Results

The overall patterns from theoretical research and cellular automata simulation are consistent, though some details differ. For instance, when $a > b$, virus propagation speed in the theoretical model exceeds that in the cellular automata simulation. The reasons are: (a) In the theoretical model, any two nodes are directly connected with full mixing, whereas in the cellular automata model, only nearby nodes can communicate directly. When all neighboring nodes of a malicious node are infected, it cannot propagate further. (b) In the cellular automata model, as propagation progresses, malicious nodes tend to cluster, and this clustering effect also hinders rapid virus spread.

4.2 Impact of Game Parameters on Virus Propagation

This study reveals virus propagation characteristics in WSN driven by attack-defense games: when the payoff a for legitimate nodes detecting viruses exceeds the loss b from infection, virus propagation continuously expands until all nodes are infected; conversely, propagation continuously contracts until the virus disappears. The explanation is as follows: From the game model in Section 2, malicious nodes propagate viruses with probability x^* while legitimate nodes detect with probability y^*. Therefore, infection probability is $x^*(1 - y^*)$ and cure probability is x^*y^*. When $a > b$, infection speed exceeds cure speed, causing virus spread; when $a < b$, infection speed is less than cure speed, causing the proportion of infected nodes to decrease.

Notably, when assessing how changes in game parameters affect propagation speed, one cannot infer based solely on one party' s possible actions but must consider both parties' actions comprehensively. For example, when $a > b$, if detection energy cost e_S increases, legitimate nodes should rationally reduce detection probability to conserve energy. However, this prompts malicious nodes to increase attack probability, causing greater losses to legitimate nodes. According to the mixed Nash equilibrium strategy, the final game outcome is that legitimate nodes maintain their detection probability while malicious nodes increase their attack probability, thereby accelerating virus propagation.

---

5 Conclusion

This paper studied virus propagation in WSN from a game-theoretic perspective, reaching the following conclusions: (a) The attack-defense game model between malicious and legitimate nodes in WSN has a mixed Nash equilibrium solution; (b) Virus propagation outcomes in WSN are related to the payoff parameters of the attack-defense game. When the payoff for legitimate nodes detecting viruses exceeds the loss from infection, the infection proportion continuously increases until all nodes are infected; conversely, the infection proportion continuously decreases until all malicious nodes disappear. These conclusions provide theoretical guidance for developing measures to suppress virus propagation in WSN.

References

[1] Qian Zhihong, Wang Yijun. Internet of Things-oriented Wireless Sensor Networks Review [J]. Journal of Electronics & Information Technology, 2013, 35(1): 215-227.

[2] Hong Feng, Chu Hongwei, Jin Zongke, et al. Review of Recent Progress on Wireless Sensor Network Applications [J]. Journal of Computer Research and Development, 2010, 47(S2): 81-87.

[3] Zhang Huanguo, Han Wenbao, Lai Xuejia, et al. Review of Cyberspace Security [J]. Scientia Sinica: Informationis, 2016, 46(2): 125-164.

[4] Li Huadeng, Li Lei, Shi Huaji, et al. Survivability evaluation in wireless sensor network [J]. Application Research of Computers, 2018, 35(8): 2450-2453.

[5] Shen Shigen, Liu Jianhua, Cao Qiying. Game theory and wireless sensor network security [M]. Beijing: Tsinghua University Press, 2016.

[6] Abdalzaher M, Seddik K, Elsabrouty M, et al. Game theory meets wireless sensor networks security requirements and threats mitigation: A survey [J]. Sensors, 2016, 16(7): 1-27.

[7] Shen Shigen, Zhou Haiping, Huang Longjun, et al. Quantal Response Equilibrium-Based Method for Preventing WSN Malware Infection [J]. Chinese Journal of Sensors and Actuators, 2017, 30(10): 1589-1595.

[8] Singh A, Awasthi A, Singh K, et al. Modeling and analysis of worm propagation in wireless sensor networks [J]. Wireless Personal Communications, 2018, 98(3), 2535-2551.

[9] Zhang Kejing, Cao Qiying, Shen Shigen. Dynamic analysis of attack and defense strategy selection for WSN based on evolutionary game[J]. Computer Applications and Software, 2017, 34(9): 132-137.

[10] Liu Yi, Lin Deyu. Defense against energy exhausting attack based on the

evolutionary game theory for the industrial wireless sensor network[J]. Measurement and Control Technology, 2018, 37(4): 58-63.

[11] Sedjelmaci H, Senouci S, Ansari N. Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: a bayesian game-theoretic methodology [J]. IEEE Trans Intelligent Transportation Systems, 2017, 18(5): 1143-1153.

[12] Zheng Rongjun, Chen Zhide, Ma Jinhua. N-worm propagation model in wireless sensor networks [J]. Journal of Computer Applications, 2015, 35(S2): 62-64.

[13] Shen S, Li H, Han R, et al. Differential game-based strategies for preventing malware propagation in wireless sensor networks [J]. IEEE Trans on Information Forensics and Security, 2014, 9(11): 1962-1973.

[14] Zhou Haiping, Cai Shaohong, Long Yan. Effect of individual difference on virus spreading efficiency [J]. Application Research of computers, 2011, 28(10): 3797-3798.

[15] Wang T, Wu Q, Wen S, et al. Propagation Modeling and Defending of a Mobile Sensor Worm in Wireless Sensor and Actuator Networks [J]. Sensors, 2017, 17(12): 139-155.

Note: Figure translations are in progress. See original paper for figures.