



基于元胞自动机和静态贝叶斯博弈的 WSN 恶意程序传染模型

张红¹, 沈士根², 吴小军¹, 曹奇英¹

(1. 东华大学, 上海 201620; 2. 绍兴文理学院, 浙江 绍兴 312000)

摘要: 基于元胞自动机理论和静态贝叶斯博弈, 研究无线传感器网络 (WSN) 中恶意程序的传染模型。首先, 依据元胞自动机理论, 建立了 WSN 中恶意程序的传染模型。然后, 基于静态贝叶斯博弈预测恶意程序的传染行为, 得到博弈双方基于贝叶斯纳什均衡 (Bayesian Nash equilibrium, BNE) 确定的最优行动, 并将其应用到上述传染模型, 从而揭示恶意程序在 WSN 中的传染动力学特征。研究表明, 该模型能揭示恶意程序在 WSN 中的传染行为, 得到各种状态传感节点的数量随时间变化的动态演化趋势, 对有效抑制 WSN 恶意程序传染有理论指导意义。

关键词: 无线传感器网络; 恶意程序传染; 时空动力学; 元胞自动机; 静态贝叶斯博弈

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019147

WSN malware infection model based on cellular automaton and static Bayesian game

ZHANG Hong¹, SHEN Shigen², WU Xiaojun¹, CAO Qiyang¹

1. Donghua University, Shanghai 201620, China

2. Shaoxing University, Shaoxing 312000, China

Abstract: The theoretical model for the malware infection in wireless sensor networks (WSN) based on cellular automaton and static Bayesian game was studied. Firstly, the malware infection model of WSN based on cellular automaton was built. Secondly, the malware infection dynamics in WSN was predicted based on the static Bayesian game, through which malware and WSN systems would determine their optimal actions by Bayesian Nash equilibrium (BNE). Then the BNE was applied to the malware infection model to study the spatiotemporal dynamics characteristics of malware infection. Research results show that the proposed model can effectively predict the infection dynamics propagation process of malware in WSN, and the evolution trend of sensor nodes in various states with time, which are of significance for people to formulate measures to reduce the propagation speed of malware.

Key words: WSN, malware infection, spatiotemporal dynamics, cellular automaton, static Bayesian game

收稿日期: 2018-12-20; 修回日期: 2019-05-12

基金项目: 国家自然科学基金资助项目 (No.61772018)

Foundation Item: The National Natural Science Foundation of China (No.61772018)

1 引言

恶意程序是对网络、系统、数据等具有恶意攻击性和严重破坏力的程序,常见的有木马、蠕虫、计算机病毒等。研究表明^[1-4],由于无线传感器网络(WSN)具有网络特性,并且传感节点具有资源有限、通信半径受限等特点,所配置的防御措施也较弱,非常容易遭受恶意程序攻击。恶意程序一旦利用网络漏洞、传感节点的系统及软硬件漏洞入侵,会快速感染周围的邻居节点,并在其中广泛传染。然后,恶意程序通过窃取或者破坏传输数据、阻塞网络等手段破坏 WSN 的正常通信,甚至采用耗尽传感节点能量的方式使其处于死亡状态,使整个 WSN 瘫痪。

WSN 所具有的自组织、动态拓扑和能量有限的特点,决定了每个传感节点在通信时有自己的决策。实际上,恶意程序在 WSN 中传染时,传感节点将采用驻留在其中的入侵检测系统对它进行防御,它们之间的行为是一种博弈行为^[5-9],因此 WSN 中的恶意程序传染问题很适合利用博弈论进行研究。目前,已有不少论文利用博弈论研究 WSN 中的安全问题。Shen 等人^[10]基于微分博弈研究了 WSN 中恶意程序的传染动力学与防御机制。王晋东等人^[11]提出了一种基于静态贝叶斯博弈针对恶意攻击的不确定性的最优防御策略选取方法,使策略选取可操作性更强。Cheng^[12]基于微分博弈提出了一种针对 WSN 攻防双方的策略具有随时间变化特点的入侵检测模型,通过求解微分博弈纳什均衡得到了最优检测策略。Chen 等人^[13]基于演化博弈提出了一种主动防御恶意程序攻击 WSN 的方法。Sedjelmaci 等人^[14]基于贝叶斯博弈提出了一种针对入侵检测系统(intrusion detection system, IDS)存在误检率的问题的检测模型,该模型能够在网络资源受限的情况下提高检测成功率。

对于 WSN 中的恶意程序传染问题,许多学者使用传染病理论、元胞自动机理论、马尔可夫链及平均场理论来研究其传染过程。然而,由于传感节点的能量有限,真实环境中 WSN 的节点只会与其周围的节点通信,因此,基于元胞自动机理论的 WSN 更接近于真实环境中的 WSN,而且研究表明元胞自动机不仅能有效克服基于平均场方法只能反映恶意程序传染的平均趋势的问题,也能克服马尔可夫链建立的随机模型缺乏空间概念、而不适合描述恶意程序传染动态特征的问题。沈士根等人^[15]利用传染病理论和马尔可夫链等理论,提出了一种针对受恶意程序传染的 WSN 可生存性评估方法。Singh 等人^[16]基于微分方程稳定性提出了一个 WSN 的蠕虫病毒传播模型,研究了通信半径和节点分布密度对蠕虫传播的影响。王小明等人^[17]基于元胞自动机研究了恶意程序在移动 WSN 中的传染行为。宋玉蓉等人^[18]研究了恶意程序在自适应网络中的传染模型。Wang 等人^[19]基于元胞自动机理论和演化博弈论,刻画了 WSN 中恶意程序的传染过程。Feng 等人^[20]基于 SRIS 模型和微分动力学理论,研究了 WSN 中蠕虫传播的动力学特征,并对其传播稳定性进行了分析。曹玉林等人^[21]根据传染病理论建立了恶意程序传播的动力学模型。赵金皓等人^[22]通过流行病理论和恶意程序的扩散方程,提出了一种节点状态时空动力学分析方法。Sayad 等人^[23]以蠕虫传播和补丁防御为例,基于扩展的流行病理论给出了一种 WSN 中的信息传播模型。Byun 等人^[24]提出了一种 WSN 基于元胞自动机(cellular automaton, CA)的节点调度算法,在保证节点间能量节约的同时,提高了网络的覆盖质量。基于元胞自动机理论的 WSN 更接近于真实环境中的 WSN,可以更精确地研究恶意程序在 WSN 中的传染动态特征。但是,上述参考文献没有反映 WSN 中基于元胞自动机的恶意程序传染模型。

本文基于静态贝叶斯博弈和元胞自动机理



论,建立了 WSN 中恶意程序的传染模型,并对其传染动力学特征进行了分析。首先,根据元胞自动机的离散特性,将 WSN 中的元素与元胞自动机的特征值进行映射,定义了元胞空间、元胞状态、元胞邻居和状态转换规则集等模型要素。然后,通过建立 WSN 系统和恶意程序之间的静态贝叶斯博弈模型,对恶意程序的传播行为进行了预测,并将所得的贝叶斯纳什均衡应用到基于元胞自动机的恶意程序传染模型,从而揭示恶意程序在 WSN 中的传染动力学特征,并证明了其模型的有效性。

2 网络模型

为简化研究,本文假设 WSN 部署在一个方形的二维空间中,传感节点在其中随机均匀分布。设 N 个传感节点随机均匀分布在一个边长为 L 的正方形区域内,该区域可以分割为多个小方格,每个小方格用二维坐标表示其空间位置,如图 1 所示。记传感节点分布密度为 λ ,则:

$$\lambda = \frac{N}{L \times L} \quad (1)$$

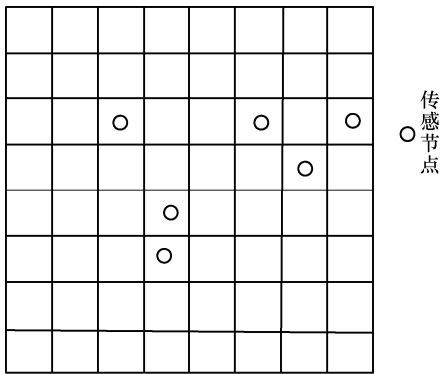


图 1 WSN 的网络模型

由于每个传感节点都能与以自身为圆心、 r 为通信半径的圆内的其他传感节点进行通信,所以每个传感节点的平均邻居节点数 M_i 可表示为:

$$M_i \approx \text{int}(\lambda \pi r^2) \quad (2)$$

其中, $\text{int}(\bullet)$ 表示取整。

3 恶意程序传染模型及传染行为预测

3.1 基于元胞自动机的恶意程序传染模型

使用元胞自动机建立恶意程序传染模型,事实上是要定义不同特征条件下(包括恶意程序攻击特性、传染环境等)元胞空间、元胞状态、元胞邻居和状态转换规则集等模型要素^[24]。

定义 1 基于二维元胞自动机(CA)建立的 WSN 恶意程序传染模型 $AC = \{C, Q, V, F\}$, 其中, C 表示元胞空间, Q 表示元胞有限状态集合, V 表示元胞邻域集合, F 表示元胞状态转换规则函数。

定义 2 元胞空间 C 是指 N 个传感节点随机均匀分布的二维空间。

本文的元胞空间是一个边长为 L 的正方形虚拟网格,设网格的每个正方形单元格边长为 1,即该正方形虚拟网格由 $L \times L$ 个小单元格组成,一个小单元格即代表一个元胞空间,网格中的 N 个传感节点即分布在其中的 N 个元胞。任意一个元胞在元胞空间的位置可以用该网格中的水平坐标 i 和垂直坐标 j 唯一标识,用 c_{ij} 表示处于 (i, j) 坐标的传感节点或元胞,则:

$$C = \{c_{i,j} | 1 \leq i, j \leq L\} \quad (3)$$

定义 3 元胞有限状态集合 $Q = \{S, I, D\}$ 。

元胞状态是指元胞在某一时刻 t 所呈现的可观察状态,包括易感状态 S 、感染状态 I 和死亡状态 D 。其中, S 是指传感节点处于容易被恶意程序感染的状态; I 是指传感节点处于已被恶意程序感染的状态; D 是指传感节点由于其能量消耗殆尽或硬件物理损坏而无法正常工作状态,此时不再参与恶意程序传染。这样, c_{ij} 元胞在 t 时刻的状态可表示为:

$$\phi_{i,j}(t) = \begin{cases} 1, & \text{元胞在} t \text{时刻处于} S \text{状态} \\ 0, & \text{元胞在} t \text{时刻处于} D \text{状态} \\ -1, & \text{元胞在} t \text{时刻处于} I \text{状态} \end{cases} \quad (4)$$

受各种因素的影响,元胞的3个状态I、S和D随着时间是不断转换的,转换概率如图2所示。处于S状态的元胞被恶意程序感染后将以 β 概率转换为I状态,后文将通过静态贝叶斯博弈求得 β 值,用以预测元胞状态的动态转换行为;由于能量消耗或者硬件损坏,处于S状态的元胞会以 η 概率转换为D状态。另外,处于I状态的元胞会以 ε 概率转换为D状态。

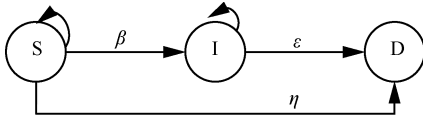


图2 传感节点状态转换关系图

定义4 元胞领域集合 $V=\{v_{i,j} | 1 \leq i,j \leq L\}$, 其中, $v_{i,j}$ 表示节点 $c_{i,j}$ 的元胞邻居。

由于元胞领域是由元胞的最大通信距离即传感节点的通信半径 r 决定的, 所以节点 $c_{i,j}$ 的邻居 $v_{i,j}$ 为:

$$v_{i,j} = \{c_{x,y} | \sqrt{(x-i)^2 + (y-j)^2} \leq r, 1 \leq x,y \leq L\} \quad (5)$$

定义5 元胞状态转换规则函数集合 $F=\{\mathcal{G}_{i,j}(t) | 1 \leq i,j \leq L\}$, 其中, $\mathcal{G}_{i,j}(t)$ 表示节点 $c_{i,j}$ 在 t 时刻的状态转换规则函数。

由于节点 $c_{i,j}$ 在 t 时刻的状态由它在 $t-1$ 时刻节点自身的状态 $\varphi_{i,j}(t-1)$ 和其邻居 $v_{i,j}$ 所处的状态 $\varphi_{v_{i,j}}(t-1)$ 共同决定, 故构造状态转换函数如下:

$$\mathcal{G}_{i,j}(t) = f(\varphi_{i,j}(t-1), \varphi_{v_{i,j}}(t-1), \iota(t)) \quad (6)$$

其中, $\iota(t)$ 表示各种状态之间的转换概率。

对于任何一个在 $t-1$ 时刻处于 S 状态的节点 n_s , 经过一个离散时间到 t 时刻后, 该节点受到处于感染状态的邻居节点的感染, 获得感染的概率会随着处于感染状态的邻居节点数目的增加而变大。在 t 时刻, 记节点 n_s 被感染的概率为 $\iota_{SI}(t)$, 不被感染的概率为 $\iota_{SS}(t)$, 死亡概率为 $\iota_{SD}(t)$, 则:

$$\iota_{SI}(t) = 1 - (1 - \beta)^k \quad (7)$$

$$\iota_{SS}(t) = 1 - \eta - [1 - (1 - \beta)^k] \quad (8)$$

$$\iota_{SD}(t) = \eta \quad (9)$$

其中, k 是 $t-1$ 时刻节点 n_s 具有已感染邻居节点的个数, 即:

$$k = \sum_{c_{x,y} \in v_{i,j}} (\varphi_{x,y}(t-1) = -1) \quad (10)$$

节点 n_s 从 $t-1$ 时刻到 t 时刻, 其状态 $\varphi_{i,j}^S(t)$ 变化如下:

$$\varphi_{i,j}^S(t) = \begin{cases} 1, & 1 - (1 - \beta)^k \leq \iota(t) \leq 1 \\ 0, & \eta \leq \iota(t) < 1 - (1 - \beta)^k \\ -1, & 0 < \iota(t) < \eta \end{cases} \quad (11)$$

对于任何一个处于 I 状态的节点 n_I , 经过一个离散时间到 t 时刻后, 记节点 n_I 保持原状态的概率为 $\iota_{II}(t)$, 死亡概率为 $\iota_{ID}(t)$, 则:

$$\iota_{II}(t) = 1 - \varepsilon \quad (12)$$

$$\iota_{ID}(t) = \varepsilon \quad (13)$$

节点 n_I 从 $t-1$ 时刻到 t 时刻, 其状态 $\varphi_{i,j}^I$ 变化如下:

$$\varphi_{i,j}^I(t) = \begin{cases} -1, & \varepsilon \leq \iota_{II}(t) < 1 \\ 0, & 0 < \iota(t) < \varepsilon \end{cases} \quad (14)$$

实际上, 恶意程序与 WSN 博弈时, 双方所拥有的信息是不对称的, 恶意程序在传染过程中无法确定传感节点所处的状态, 而恶意程序的策略则是双方的共有信息。WSN 和恶意程序将会选择各自的策略进行博弈, 逻辑上可以认为双方是同时行动的。因而, WSN 和恶意程序双方选择策略的过程可以看作一个静态贝叶斯博弈, 博弈的结果用来预测恶意程序的传染行为。

3.2 恶意程序传染行为的预测

本文使用博弈论工具对恶意程序在 WSN 中的传染行为进行建模^[25], 构建了基于静态贝叶斯博弈的恶意程序传染 (malware infection based on static Bayesian game, MISBG) 模型。该模型不仅能模拟 WSN 系统和恶意程序之间的攻防行为, 也能合理有效地预测恶意程序的传染行为。

定义6 模型 MISBG 是一个五元组



$G=(B,\Theta,P,A,\mu)$ ，其中：

- $B = \{\text{“传感节点”参与者 } a, \text{“入侵检测系统”参与者 } b\}$ 是一个包含两个参与者的集合。
- $\Theta = \Theta_a \times \Theta_b$ ，其中 $\Theta_a = \{\theta_a^S, \theta_a^I\}$ 是参与者 a 的类型空间， θ_a^S 表示 WSN 中处于 S 状态的传感节点， θ_a^I 表示 WSN 中处于 I 状态的传感节点，已被恶意程序感染，会传染周围的邻居节点； $\Theta_b = \{\theta_b\}$ 是参与者 b 的类型空间， θ_b 表示 WSN 中的入侵检测系统。
- $P: \Theta \mapsto [0,1]$ 是参与者 a 的推断（先验概率）。 $P=(\rho, 1-\rho)$ ，其中 ρ 表示 WSN 中处于 I 状态的传感节点的概率， $1-\rho$ 表示 WSN 中处于 S 状态的传感节点的概率。
- $A = A_a \times A_b$ ，其中 $A_a = \{A_a(\theta_a^I) = \{\text{infect, non-infect}\}, A_a(\theta_a^S) = \{\text{non-infect}\}\}$ 是参与者 a 可以选择的动作集合， $A_b = \{A_b(\theta_b) = \{\text{defend, non-defend}\}\}$ 是参与者 b 可选择的动作集合。
- $\mu = (\mu_a, \mu_b)$ ，其中 $\mu_a: A \times \Theta \mapsto \mathbb{R}$ 是参与者 a 的收益函数， $\mu_b: A \times \Theta \mapsto \mathbb{R}$ 是参与者 b 的收益函数。 μ_a 和 μ_b 的支付矩阵如图 3 所示。

		defend	non-defend
infect		$-\alpha R + (1-\alpha)\phi - C_1, (2\alpha-1)R - C_D$	$\phi - C_1, -R$
non-infect		$\omega R, -\omega R - C_D$	R, R

(a) 参与者 a 是 I 状态的节点

		defend	non-defend
non-infect		$\omega R, -\omega R - C_D$	R, R

(b) 参与者 a 是 S 状态的节点

图 3 MISBG 模型的支付矩阵

为描述模型 MISBG 的支付矩阵，记 α 和 ω 分别为入侵检测系统的检测率和误报率， C_D 为入侵检测系统防御恶意程序传染所消耗的能量， C_1 为处于 I 状态的传感节点传染恶意程序所消耗的能量。为强化节点之间的有效合作，本文设置了激

励能量 $R(R > C_D)$ 。处于 I 状态的传感节点如果传染恶意程序时，被检测到，它将损失一份激励能量，而入侵检测系统则收获一份激励能量；若没有被检测到，它将收获能量 $\phi(\phi > R + C_1)$ ，而入侵检测系统将损失一份激励能量。相反，如果该传感节点不传染恶意程序，它和入侵检测系统都将收获一份激励能量。

当参与者 a 是 I 状态的节点时，若双方参与者采取“纯策略对”(infect, defend)，对参与者 a 而言，若被成功检测，将损失 $-\alpha R$ ；否则，将收获 $(1-\alpha)\phi$ ，因此，其支付为：

$$u_{ID}^a = -\alpha R + (1-\alpha)\phi - C_1 \quad (15)$$

对参与者 b 而言，成功检测恶意程序将收获 αR ，没有成功检测将损失 $-(1-\alpha)R$ ，因此，其支付为：

$$u_{ID}^b = (2\alpha-1)R - C_D \quad (16)$$

若双方参与者采取“纯策略对”(infect, non-defend)，对参与者 a 而言，其支付为：

$$u_{IN}^a = \phi - C_1 \quad (17)$$

而参与者 b ，其支付为：

$$u_{IN}^b = -R \quad (18)$$

若双方参与者采取“纯策略对”(non-infect, defend)，对参与者 a 而言，其支付为：

$$u_{ND}^a = \omega R \quad (19)$$

而参与者 b 的支付为：

$$u_{ND}^b = -\omega R - C_D \quad (20)$$

若双方参与者采取“纯策略对”(non-infect, non-defend)，对参与者 a 而言，其支付为：

$$u_{NN}^a = R \quad (21)$$

而参与者 b 的支付为：

$$u_{NN}^b = R \quad (22)$$

当参与者 a 是 S 状态的节点时，其支付可根据上述计算式类推。

3.3 WSN 和恶意程序博弈的贝叶斯纳什均衡

本文使用海萨尼转换求解贝叶斯均衡。具体转换时,引入虚拟参与者——“自然”(T),由“自然”T先行动,以随机概率 ρ 选择参与人 a 的类型,这样对于参与人 b ,参与人 a 的类型就由不完全信息变成了完全不完美的信息。入侵检测系统和传感节点之间的博弈经过海萨尼转换就可以用如图4所示的博弈树表述。

WSN 和恶意程序博弈的过程分析如下。

定理 1 当 $\rho < \frac{C_D + R(1+\omega)}{(2+\omega+\alpha)R}$ 成立时,

MISBG 模型存在纯策略贝叶斯均衡。

证明: (1) 当参与者 a 选择纯策略($A_a(\theta_a^S)=\{\text{non-infect}\}$, $A_a(\theta_a^I)=\{\text{infect}\}$),意味着当传感节点属于易感节点时,总是选择动作 infect,而当其属于感染节点时,总是选择动作 non-infect。因此,对参与者 b 而言,选择动作 defend 和 non-defend 的期望收益分别是:

$$E_{\mu_b}(\text{defend}) = \rho((2\alpha-1)R - C_D) - (1-\rho)(\omega R + C_D) \quad (23)$$

以及:

$$E_{\mu_b}(\text{non-defend}) = -\rho R + (1-\rho)R \quad (24)$$

如果 $E_{\mu_b}(\text{defend}) > E_{\mu_b}(\text{non-defend})$, 即:

$$\rho > \frac{C_D + R(1+\omega)}{(2\alpha+\omega+1)R} \quad (25)$$

那么入侵检测系统的最优策略是 defend。然而,当入侵检测系统选择动作 defend,传感节点

的最优策略不再是 infect 时,这是因为不等式:

$$\omega R > -\alpha R + (1-\alpha)\phi - C_1 \quad (26)$$

恒成立。因此, ($A_a(\theta_a^S)=\{\text{non-infect}\}$, $A_a(\theta_a^I)=\{\text{infect}\}$, $A_b(\theta_b)=\{\text{defend}\}$) 不是 MISBG 的纯策略贝叶斯均衡。

如果 $E_{\mu_b}(\text{defend}) < E_{\mu_b}(\text{non-defend})$, 即:

$$\rho < \frac{C_D + R(1+\omega)}{(2\alpha+\omega+1)R} \quad (27)$$

那么入侵检测系统的最优策略是 non-defend。然而,当入侵检测系统选择动作,传感节点的最优策略是 non-defend,这是因为不等式:

$$\phi - C_1 > R \quad (28)$$

恒成立。因此, ($A_a(\theta_a^S)=\{\text{non-infect}\}$, $A_a(\theta_a^I)=\{\text{infect}\}$, $A_b(\theta_b)=\{\text{non-defend}\}$) 是 MISBG 的纯策略贝叶斯均衡。

(2) 当参与者选择纯策略 ($A_a(\theta_a^S)=\{\text{non-infect}\}$, $A_a(\theta_a^I)=\{\text{non-infect}\}$), 意味着不管传感节点属于易感节点还是感染节点,总是选择动作 non-infect,而对于入侵检测系统而言,non-infect 动作的最优响应是 non-defend,而对于传感节点属于感染节点而言,针对入侵检测系统动作 non-defend 的最优响应是动作 infect,这与纯策略 ($A_a(\theta_a^S)=\{\text{non-infect}\}$, $A_a(\theta_a^I)=\{\text{non-infect}\}$) 相互矛盾,因此, ($A_a(\theta_a^S)=\{\text{non-infect}\}$, $A_a(\theta_a^I)=\{\text{non-infect}\}$, $A_b(\theta_b)=\{\text{non-defend}\}$) 不是 MISBG 的纯策略贝叶斯均衡。

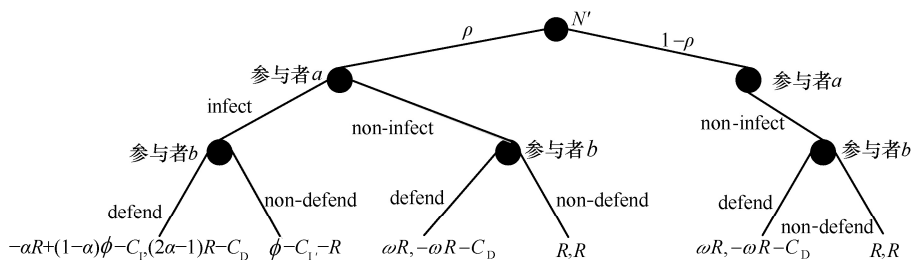


图4 入侵检测系统和传感节点的博弈树



综上所述, 当:

$$\rho < \frac{C_D + R(1+\omega)}{(2\alpha + \omega + 1)R} \quad (29)$$

成立时, MISBG 存在纯策略贝叶斯均衡 ($A_a(\theta_a^S) = \{\text{non-infect}\}$, $A_a(\theta_a^I) = \{\text{infect}\}$, $A_b(\theta_b) = \{\text{non-defend}\}$)。这意味着传感节点属于易感节点时总是选择动作 non-infect, 而属于感染节点时总是选择动作 infect, 入侵检测系统总是选择动作 non-defend。证毕。

虽然 MISBG 存在纯策略贝叶斯均衡, 但这与实际的防御要求不符, 因为根据定理 1, 入侵检测系统总是选择动作 non-defend, 这就是说传感节点传染恶意程序不会被入侵检测系统阻拦。因此仅得到纯策略贝叶斯均衡是不够的, 必须要找到能用于检测恶意程序的混合策略贝叶斯均衡。

定理 2 当 $\rho > \frac{C_D + R(1+\omega)}{(2\alpha + \omega + 1)R}$ 成立时, MISBG 模型存在混合策略贝叶斯均衡。

证明: 显然, 只有条件 $\rho > \frac{C_D + R(1+\omega)}{(2\alpha + \omega + 1)R}$ 成立时, MISBG 模型才有可能存在混合策略贝叶斯均衡。

设传感节点 θ_a^I 的混合策略为 $\sigma_a = (\zeta, 1-\zeta)$, 那么, 入侵检测系统选择动作 defend 和 non-defend 的期望收益分别是:

$$E\mu_b(\text{defend}) = \rho\zeta((2\alpha - 1)R - C_D) + \rho(1-\zeta)(-\omega R - C_D) + (1-\rho)(-\omega R - C_D) \quad (30)$$

$$E\mu_b(\text{non-defend}) = -\rho\zeta R + \rho(1-\zeta)R + (1-\rho)R \quad (31)$$

在传感节点 θ_a^I 采取最优混合策略 σ_a^* 前提下, 由入侵检测系统选择动作 defend 和 non-defend 的无差异性可以得到:

$$E\mu_b(\text{defend}) = E\mu_b(\text{non-defend}) \quad (32)$$

因此, 入侵检测系统采取的最优混合策略是:

$$\sigma_b^* = \frac{(\omega+1)R + C_D}{\rho R(1+\omega+2\alpha)} \quad (33)$$

设入侵检测系统的混合策略为 $\sigma_b = (\zeta, 1-\zeta)$, 那么参与者 a 采取动作 infect 和 non-infect 期望收益分别是:

$$E\mu_a(\text{infect}) = \rho\zeta(-\alpha R + (1-\alpha)\phi - C_1) + \rho(1-\zeta)(\phi - C_1) \quad (34)$$

$$E\mu_a(\text{non-infect}) = \rho\zeta\omega R + \rho(1-\zeta)R + (1-\rho)\zeta\omega R + (1-\rho)(1-\zeta)R \quad (35)$$

在入侵检测系统采取最优混合策略 σ_b^* 的情况下, 由参与者 a 采取动作 infect 和 non-infect 的无差异性可以得到:

$$E\mu_a(\text{infect}) = E\mu_a(\text{non-infect}) \quad (36)$$

因此, 传感节点 θ_a^I 的最优混合策略为:

$$\sigma_a^* = \frac{\rho(\phi - C_1) - R}{\rho\alpha(R + \phi) - (1-\omega)R} \quad (37)$$

综上所述, MISBG 模型存在混合策略完美贝叶斯均衡 (σ_a^*, σ_b^*), 证毕。

定理 2 表示在 MISBG 模型中, 两个理性参与者传感节点和入侵检测系统在博弈过程中, 将选择最优策略对 (σ_a^*, σ_b^*)。随着传感节点和入侵检测系统博弈的不断推进, 它们将根据定理 2 选择最优的动作以获取最大的利益。

4 仿真结果及分析

本文实验仿真和数据分析通过 VC6.0 和 MATLAB R2013a 完成, 其中仿真的关键参数设置为: 正方形网络区域大小为 500 m×500 m, 无线传感节点共 3 000 个, 每次实验仿真 100 步, 入侵检测系统检测率 $\alpha=0.7$, 误报率 $\omega=0.2$, 入侵检测系统防御的成本 $C_D=40$, 传感节点发起传染的成本 $C_1=40$, 奖励收益 $R=100$, 传感节点如果传染恶意程序没有被检测到的收益 $\phi=150$, 易感节点的正常死亡概率 $\eta=0.005$, 感染节点的死亡概率为 $\varepsilon=0.008$ 。实验中通过变换传感节点的通信半径 r , 恶意传感节点的初始数

量,求解处于 I 状态的传感节点的数量随时间的演化曲线。

图 5 给出了在恶意程序的传染过程中,传感节点的通信半径分别为 6 m、8 m、10 m 时,处于 I 状态的传感节点的数量变化趋势。通过图 5 可以分析得到,传感节点的通信半径越大,恶意程序传染的范围越大,传染的速度越快,也就是说,每个时间步内被感染传感节点的数量增加越多。此外,恶意程序的传染过程可分为传染加速、传染平稳和传染消亡 3 个阶段。通信半径越大,传染加速期越长,传染的平稳期越短,被感染传感节点数量减少得越快。

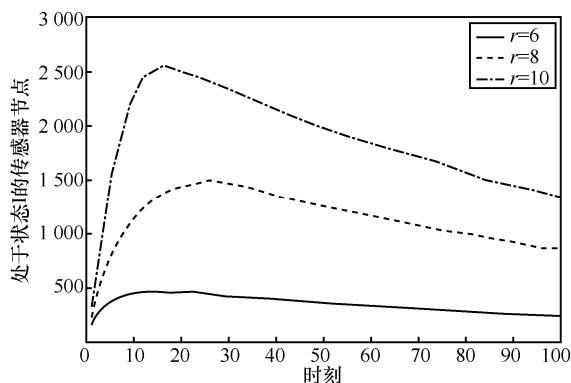


图 5 通信半径对恶意程序传染的影响

图 6 给出了在恶意程序的传染过程中,WSN 中处于 I 状态的传感节点的初始数量分别为 50 个、100 个、150 个时,处于 I 状态传感节点的数量变化趋势。通过图 6 可以分析得到,感染节点的初始数量越大,恶意程序传染得越快,每个时间步内传感节点被感染的数量增加得越快,但是,传染加速期和传染平缓期都变短,被感染传感节点数量减少得越快。

图 7 给出了传感节点和入侵检测系统之间博弈时,入侵检测系统是否实施防御,对处于 I 状态的传感节点的数量变化趋势。通过图 7 可以分析得到,当入侵检测系统防御时被感染的传感节点较少,而且处于 I 状态的传感节点会提前进入消亡阶段。

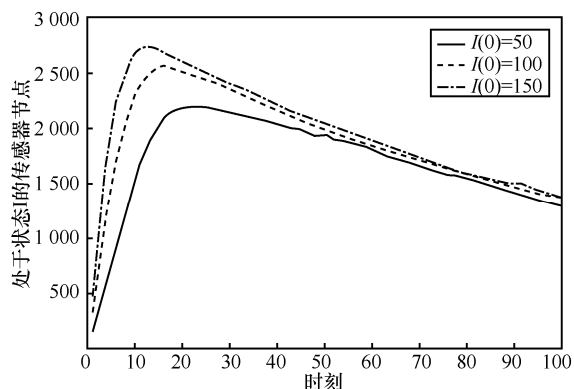


图 6 感染节点的初始数量对恶意程序传染的影响

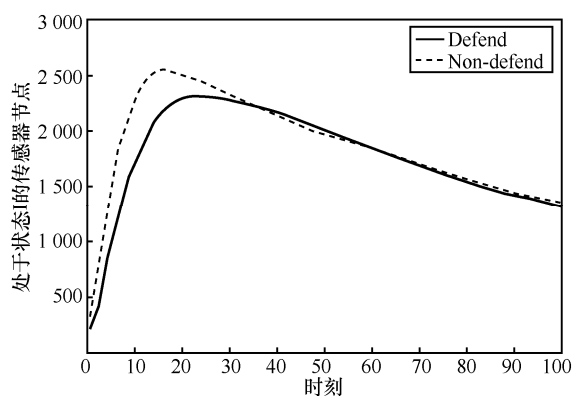


图 7 入侵检测系统的防御策略对恶意程序传染的影响

图 8 给出了在恶意程序的传染过程中,WSN 中 3 种状态的传感节点的数量变化趋势。通过图 8 可以分析得到,状态 I 和状态 S 的传感节点的数量变化趋势相似,传染的 3 个过程比较明显,而且基本在同一时刻,两种状态的传感节点迅速减少,死亡节点迅速增加,恶意程序处于消亡阶段。

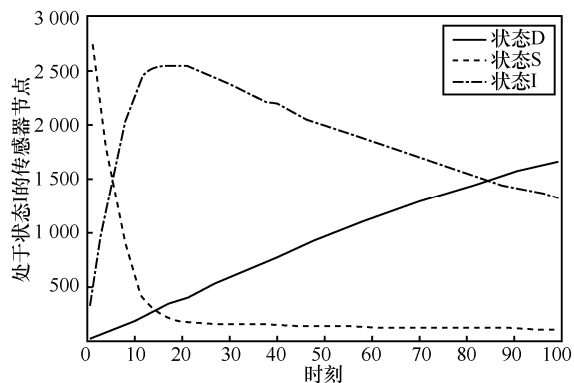


图 8 感染节点的数量随时间的变化曲线



5 结束语

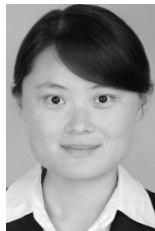
本文针对 WSN 中恶意程序的传染问题,提出了基于静态贝叶斯博弈和元胞自动机理论的恶意程序传染模型,研究恶意程序在 WSN 中的传染行为,并对恶意程序的传染动力学特征进行分析。实验分析了传感节点的通信半径、感染节点的初始数量、入侵检测系统的策略等因素对恶意程序在 WSN 中传染行为的影响。研究表明,该模型可以更有效地描述恶意程序在 WSN 中的传染过程以及各种状态的传感节点随时间的动态演化趋势,对有效抑制 WSN 中恶意程序的传染具有理论指导意义。

参考文献:

- [1] 沈士根, 黄龙军, 周海平, 等. 面向恶意程序传播的异质 WSN 稳态可用度评估[J]. 传感技术学报, 2017, 30(7): 1100-1105.
SHEN S G, HUANG L J, ZHOU H P, et al. Steady-state availability evaluation for heterogeneous WSN under malware infection[J]. Chinese Journal of Sensors and Actuators, 2017, 30(7): 1100-1105.
- [2] 沈士根, 周海平, 黄龙军, 等. 基于最优反应均衡的传感网恶意程序传播抑制方法[J]. 传感技术学报, 2017, 30(10): 1589-1595.
SHEN S G, ZHOU H P, HUANG L J, et al. Quantal response equilibrium-based method for preventing WSN malware infection[J]. Chinese Journal of Sensors and Actuators, 2017, 30(10): 1589-1595.
- [3] 沈士根, 范恩, 胡珂立, 等. 面向恶意程序传播的传感网可靠度评估[J]. 电子学报, 2018, 46(1): 75-81.
SHEN S G, FAN E, HU K L, et al. Reliability evaluation for WSN with malware spread[J]. Acta Electronica Sinica, 2018, 46(1): 75-81.
- [4] 沈士根, 冯晟, 周海平, 等. 基于云计算和动态贝叶斯博弈的 WSN 恶意程序传播优化抑制方法[J]. 电信科学, 2018, 34(9): 78-86.
SHEN S G, FENG S, ZHOU H P, et al. Optimal approach of suppressing WSN malware propagation based on cloud computing and dynamic Bayesian game[J]. Telecommunications Science, 2018, 34(9): 78-86.
- [5] ZHU L, ZHAO H. Dynamical analysis and optimal control for a malware propagation model in an information network[J]. Neurocomputing, 2015(149): 1370-1386.
- [6] WANG Y, WEN S, XIANG Y, et al. Modeling the propagation of worms in networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2014, 16(2): 942-960.
- [7] HOSSEINI S, AZGOMI M A, RAHMANI A T. Malware propagation modeling considering software diversity and immunization[J]. Journal of Computational Science, 2016(13): 49-67.
- [8] MOHI M, MOVAGHAR A, ZADEH P M. A Bayesian game approach for preventing DoS attacks in wireless sensor networks[C]//2009 WRI International Conference on Communications and Mobile Computing, Jan 6-8, 2009, Kunming, China. Piscataway: IEEE Press, 2009: 507-511.
- [9] 沈士根, 刘建华, 曹奇英. 博弈论与无线传感器网络安全[M]. 北京: 清华大学出版社, 2016.
SHEN S G, LIU J H, CAO Q Y. Game theory and wireless sensor network security[M]. Beijing: Tsinghua University Press, 2016.
- [10] SHEN S, LI H, HAN R, et al. Differential game-based strategies for preventing malware propagation in wireless sensor networks[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(11): 1962-1973.
- [11] 王晋东, 余定坤, 张恒巍, 等. 静态贝叶斯博弈主动防御策略选取方法[J]. 西安电子科技大学学报, 2016(1): 144-150.
WANG J D, YU D K, ZHANG H W, et al. Active defense strategy based on the static Bayesian game[J]. Journal of Xidian University, 2016(1): 144-150.
- [12] CHENG Z. A differential game model between intrusion detection system and attackers for wireless sensor networks[J]. Wireless Personal Communications, 2016, 90(3): 1211-1219.
- [13] CHEN Z, QIAO C, QIU Y, et al. Dynamics stability in wireless sensor networks active defense model [J]. Journal of Computer and System Sciences, 2014, 80(8): 1534-1548.
- [14] SEDJELMACI H, SENOUCI S, ANSARI N. Intrusion detection and ejection framework against lethal attacks in UAV-aided network: a Bayesian game-theoretic methodology [J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(5): 1143-1153.
- [15] 沈士根, 黄龙军, 范恩, 等. 受恶意程序传染的 WSN 可生存性评估[J]. 传感技术学报, 2016, 29(7): 1083-1089.
SHEN S G, HUANG L J, FAN E, et al. Survivability evaluation for WSN under malware infection[J]. Chinese Journal of Sensors and Actuators, 2016, 29(7): 1083-1089.
- [16] SINGH A, AWASTHI A, SINGH K, et al. Modeling and analysis of worm propagation in wireless sensor network [J]. Wireless Personal Communications, 2018, 98(3): 2535-2551.
- [17] 王小明, 李成博, 李英殊. 移动无线传感网恶意数据包传染随机模型[J]. 电子与信息学报, 2013, 35(6): 1290-1297.
WANG X M, LI C B, LI Y S. A stochastic model of malicious data packet propagation in mobile wireless sensor networks[J]. Journal of Electronics & Information Technology, 2013, 35(6): 1290-1297.
- [18] 宋玉蓉, 蒋国平, 徐加刚. 一种基于元胞自动机的自适应网络病毒传播模型[J]. 物理学报, 2011(12): 115-124.
SONG Y R, JIANG G P, XU J G. An epidemic spreading model

- in adaptive networks based on cellular automata[J]. Acta Physica Sinica, 2011(12): 115-124.
- [19] WANG Y, LI D, DONG N. Cellular automata malware propagation model for WSN based on multi-player evolutionary game[J]. IET Networks, 2018, 7(3): 129-135.
- [20] FENG L, SONG L, ZHAO Q, et al. Modeling and stability analysis of worm propagation in wireless sensor network[J]. Mathematical Problems in Engineering, 2015: 1-8.
- [21] 曹玉林, 赵焱鑫, 王小明. 基于元胞自动机的自适应网络断边重连策略研究[J]. 计算机应用研究, 2016(8): 2475-2478.
- CAO Y L, ZHAO Y X, WANG X M. Research on reconnecting strategy of adaptive networks based on cellular automata[J]. Application Research of Computers, 2016(8): 2475-2478.
- [22] 赵金皓, 曹奇英, 沈士根. 受到恶意程序攻击的 MWSN 节点状态时空动力学分析[J]. 计算机应用与软件, 2018(6): 122-128.
- ZHAO J H, CAO Q Y, SHEN S G. Spatiotemporal dynamics analyses of mobile sensor nodes attacked by malware[J]. Computer Applications and Software, 2018(6): 122-128.
- [23] SAYAD H M, WEN S, XIANG Y, et al. On the race of worms and patches: modeling the spread of information in wireless sensor networks[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(12): 2854-2865.
- [24] BYUN H, YU J. Cellular-automaton-based node scheduling control for wireless sensor networks[J]. IEEE Transactions on Vehicular Technology, 2014, 63(8): 3892-3899.
- [25] 刘玉岭, 冯登国, 吴丽辉, 等. 基于静态贝叶斯博弈的蠕虫攻防策略绩效评估[J]. 软件学报, 2012(3): 712-723.
- LIU Y L, FENG D G, WU L H, et al. Performance evaluation of worm attack and defense strategies based on static Bayesian game[J]. Journal of Software, 2012(3): 712-723.

[作者简介]



张红 (1984-), 女, 东华大学计算机科学与技术学院博士生, 主要研究方向为无线传感器网络、网络空间安全、博弈论。



沈士根 (1974-), 男, 博士, 绍兴文理学院计算机科学与工程系教授, 主要研究方向为无线传感器网络、物联网、博弈论。



吴小军 (1978-), 男, 东华大学信息科学与技术学院博士生, 主要研究方向为无线传感器网络、智能系统。



曹奇英 (1960-), 男, 博士, 东华大学计算机科学与技术学院教授、博士生导师, 主要研究方向为普适计算、智能信息处理。