



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

沈士根¹, 冯晟¹, 周海平¹, 黄龙军¹, 胡珂立¹, 曹奇英²

(1. 绍兴文理学院计算机科学与工程系, 浙江 绍兴 312000;

2. 东华大学计算机科学与技术学院, 上海 201620)

摘要: 为有效地应用入侵检测系统检测 WSN (wireless sensor network, 无线传感网络) 恶意程序从而抑制 WSN 恶意程序传播, 在考虑 WSN 节点资源有限和云计算平台资源几乎无限的现状基础上, 借助云计算平台提出 WSN 入侵检测网络结构。依据传感节点和 WSN 入侵检测代理之间博弈过程的分析, 使用动态贝叶斯博弈建立了考虑 WSN 入侵检测代理监控数据发送能耗和传感节点隐私保护需求的 WSN 恶意程序传播抑制博弈模型。依据建立的博弈类型, 并基于精炼贝叶斯均衡提出抑制 WSN 恶意程序传播的优化策略, 并给出具体的算法。实验分析了影响 WSN 入侵检测代理选择优化策略的因素, 为具体应用提供了实验依据。

关键词: WSN; 恶意程序; 入侵检测系统; 云计算; 动态贝叶斯博弈

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018259

Optimal approach of suppressing WSN malware propagation based on cloud computing and dynamic Bayesian game

SHEN Shigen¹, FENG Sheng¹, ZHOU Haiping¹, HUANG Longjun¹, HU Keli¹, CAO Qiying²

1. Department of Computer Science and Engineering, Shaoxing University, Shaoxing 312000, China

2. College of Computer Science and Technology, Donghua University, Shanghai 201620, China

Abstract: To apply intrusion detection system (IDS) efficiently so as to suppress WSN malware propagation, a cloud-based network infrastructure for realizing functions of WSN IDS was presented, considering the real basis that the resources of WSN nodes were limited whilst the resources of cloud computing platform were almost unlimited. Based on the analysis of the game process between a sensor node and the corresponding WSN IDS agent, a WSN-malware-propagation-suppression game model was constructed by employing the dynamic Bayesian game, and the requirements of energy consumption in sending monitored data and privacy protection for sensor nodes were satisfied. According to the proposed game type and refined Bayesian equilibrium, the optimal strategy for suppressing WSN malware was proposed as well the algorithm for actual application was given. The factors that influence WSN IDS agents to select their optimal strategies were analyzed, and the experimental foundation was provided for the application of the proposed approach.

Key words: wireless sensor network, malware, intrusion detection system, cloud computing, dynamic Bayesian game

收稿日期: 2018-03-11; 修回日期: 2018-09-10

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

当前, WSN 恶意程序传播已成为网络空间安全研究的重要内容^[1-7], 这些恶意程序通过感染传感节点、插入欺骗数据产生错误感知信息、故意增加传感节点能耗等方式干扰和破坏整个 WSN 的正常通信, 对整个 WSN 的数据安全造成极大破坏^[8-9]。为抑制 WSN 恶意程序的传播, 一种通用的方法是利用入侵检测系统 (intrusion detection system, IDS) 检测恶意程序并给出抑制恶意程序传播的措施^[10-15]。

然而, 要将传统 IDS 技术应用于 WSN 面临诸多问题。与传统安装 IDS 的节点具有丰富的计算资源不同, 传感节点通常只具有有限的能量、存储和计算资源, 因此, 如何处理和存储入侵检测代理监测传感节点产生的大量监控数据成为首要问题。此外, WSN 普遍具有的拓扑异质性也给入侵检测代理部署带来新的挑战。

云计算的服务模式在计算、存储、安全等方面提供了一种新的体系结构^[16], 其中, “IDS as a service” (IDSaaS)^[17-18]服务能够在云计算平台中检测监控数据并判断恶意程序的恶意行为。借助这种计算模式可以整合具有拓扑结构异质性的 WSN, 以及几乎无限量地扩充数据存储和计算资源, 从而有效解决 WSN 部署入侵检测代理和入侵检测计算问题。然而, 由于使用这种模式需要将监控数据发送到云计算平台进行检测, 不可避免地会产生如何考虑在 WSN 入侵检测代理监控数据发送能耗和传感节点隐私保护的前提下最大化抑制 WSN 恶意程序传播的决策问题。

博弈论考虑参与者的预测行为和实际行为已成为探究实现参与者利益最大化优化策略的理论工具, 该理论工具同样适用于探究最大化抑制 WSN 恶意程序传播策略的优化。王晋东等人^[19]在考虑防御者类型基础上使用静态贝叶斯博弈给出了一种优化防御策略。刘玉岭等人^[20]同样使用

静态贝叶斯博弈, 通过建立恶意程序攻防策略绩效评估模型为抑制恶意程序传播提供借鉴。沈士根等人^[21]利用微分博弈给出一种抑制在线社交网络恶意程序传播的方法。张恒巍等人^[22]针对动态攻防过程具有的信息不完全性和多阶段性的特点, 建立了多阶段攻防信号博弈模型, 并给出了优化防御策略。黄健明等人^[23]使用非合作演化博弈给出了基于演化稳定策略的优化防御策略。Spyridopoulos 等人^[24]考虑恶意程序传播的影响, 使用完全信息静态博弈提出了一种优化抑制策略。Yuan 等人^[25]使用 Stackelberg 博弈给出了一种具有弹性控制的优化策略。周恒杰等人^[26]使用不完全信息动态博弈针对多信道无线网络给出了优化的抗干扰传输策略。除上述可借鉴应用于探究抑制 WSN 恶意程序传播优化策略的博弈类型外, 其他典型的博弈类型还包括重复博弈^[27]、粗糙集博弈^[28]、演化泊松博弈^[29]等。

本文借助云计算给出 WSN 入侵检测网络结构, 并基于动态贝叶斯博弈提出一种用于抑制 WSN 恶意程序传播的优化方法。首先, 考虑 WSN 节点资源有限和云计算平台资源几乎无限现状, 给出一种新的 WSN 入侵检测代理工作模式; 其次, 依据 WSN 入侵检测代理监控数据发送能耗和传感节点隐私保护需求, 分析传感节点和 WSN 入侵检测代理之间的博弈过程, 基于动态贝叶斯博弈思想建立 WSN 恶意程序传播抑制博弈模型; 最后, 基于精炼贝叶斯均衡思想给出抑制 WSN 恶意程序传播的优化策略, 并给出实际应用的算法。

2 网络体系结构

在 WSN 的节点中部署入侵检测代理, 一般包括 3 种模式: 集中式、分布式和混合式^[10]。其中, 集中式将入侵检测代理部署在汇聚 (sink) 节点上, 这种模式的好处是能在能量充沛的汇聚节点上集中处理监控数据, 但传感节点需要传送所有的监控数据到汇聚节点, 因此通信负载加重; 分布式



将入侵检测代理部署在所有传感节点上, 这种模式能有效降低通信负载但也加重了所有传感节点用于完成入侵检测代理工作的能量消耗; 混合式将选择部分传感节点(如采用 watchdog 技术的节点)部署入侵检测代理, 这些节点通常监控一块区域(如采用分簇管理的 WSN 中可考虑按簇划分区域), 既担任感知节点又担任监控节点。

WSN 网络体系结构如图 1 所示, 借助云计算强大的存储和运算能力, 本文提出一种与传统模式不同的入侵检测代理工作模式。该模式在所有的传感节点中部署入侵检测代理, 但这些入侵检测代理不是一直处于工作状态, 只有被选择为中继节点的传感节点上的入侵检测代理才会被触发并启动, 并且入侵检测代理的主要工作是收集监控数据, 而入侵检测这项耗费大量计算和能量资源的工作则由云计算平台中的 IDSaaS 完成。

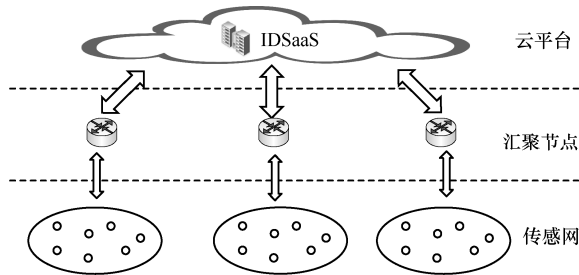


图 1 网络体系结构

在图 1 中, 当入侵检测代理收集到监控数据后, 面临是否提交监控数据, 从而抑制 WSN 恶意程序传播的决策问题。一方面, 入侵检测代理只有提交监控数据才可能检测到恶意程序的传播并给出抑制其传播的措施; 另一方面, 入侵检测代理在提交监控数据时将消耗用于数据发送的能量, 同时将泄露包含在监控数据中的隐私数据(如节点位置信息等)。因此, 接下来通过建立 WSN 恶意程序传播抑制博弈模型来寻求优化策略, 以便在考虑 WSN 入侵检测代理监控数据发送能耗和传感节点隐私保护因素的基础上, 最大化抑制 WSN 恶意程序的传播。

3 WSN 恶意程序传播抑制博弈模型

定义 1 在考虑 WSN 入侵检测代理监控数据发送能耗和传感节点隐私保护的基础上, 将 WSN 恶意程序传播抑制博弈模型表示为一个五元组 $\Xi = (\Delta, \Phi, \Lambda, \Theta, \Psi)$, 其中:

- $\Delta = \{\text{传感节点 } i, \text{WSN 入侵检测代理 } j\}$ 为博弈参与者的集合;
- $\Phi = \Phi_i \times \Phi_j$ 为参与者类型空间的笛卡尔积, $\Phi_i = \{\phi_i^N, \phi_i^S, \phi_i^M\}$ 为传感节点 i 的类型空间, $\Phi_j = \{\phi_j\}$ 为 WSN 入侵检测代理 j 的类型空间;
- $\Lambda = \Lambda_i \times \Lambda_j$ 为参与者动作空间的笛卡尔积, $\Lambda_i = \Lambda_i(\phi_i^N) \cup \Lambda_i(\phi_i^S) \cup \Lambda_i(\phi_i^M)$ 为传感节点 Ξ 的动作空间, $\Lambda_i(\phi_i^N) = \{\text{合作 (Collaborate, } C)\}$ 为正常传感节点的动作空间, $\Lambda_i(\phi_i^S) = \{\text{合作 (Collaborate, } C), \text{分组丢失 (Drop, } D)\}$ 为自私传感节点的动作空间, $\Lambda_i(\phi_i^M) = \{\text{合作 (Collaborate, } C), \text{分组丢失 (Drop, } D), \text{传播 (Propagate, } P)\}$ 为恶意传感节点的动作空间。 $\Lambda_j = \{\text{提交 (Submit, } \tilde{S}), \text{空闲 (Inactivate, } I)\}$ 为 WSN 入侵检测代理 Ξ 的动作空间;
- $\forall z \in \Delta, \forall x \in \Lambda_i(\phi_i^N), \forall \tilde{x} \in \Lambda_i(\phi_i^S), \forall \bar{x} \in \Lambda_i(\phi_i^M), \forall y \in \Lambda_j, \Theta = [o_{xy}^z] \cup [o_{\tilde{xy}}^z] \cup [o_{\bar{xy}}^z]$ 为博弈参与者的支付矩阵, 其中, $o_{xy}^z, o_{\tilde{xy}}^z, o_{\bar{xy}}^z$ 分别表示传感节点 i 选择动作 $x, \tilde{x}, \bar{x}$, 而 WSN 入侵检测代理 j 选择动作 y 后参与者 z 得到的支付值;
- $\Psi = \{(p_1(\phi_i^N), p_1(\phi_i^S), p_1(\phi_i^M)), (p_2(\phi_i^N), p_2(\phi_i^M)), \dots\}$ 为传感节点类型空间分布概率的集合, 其中, $p_1(\phi_i^N), p_1(\phi_i^S), p_1(\phi_i^M)$ 分别表示传感节点在时刻 $t (t \in \mathbb{Z}^+)$ 属于传感节点类型 $\phi_i^N, \phi_i^S, \phi_i^M$ 的概率。

本文根据传感节点的实际情况, 将传感节点 i 的类型分为正常 (N)、自私 (S) 和恶意 (M)

3 种类型,而 WSN 入侵检测代理 j 只有一种类型。由于传感节点 j 在检测前的类型未知,按博弈论的说法,其信息对 WSN 入侵检测代理 j 而言属于私有信息,而 WSN 入侵检测代理 j 的类型对双方而言是公共信息。对于一个类型为正常的传感节点,可被用于感知信息、转发数据等,这些行为统一归纳为一种动作“合作(C)”；对于一个自私传感节点,由于数据转发会导致自身的能量消耗,因此它除具有正常节点的动作外,还有可能为减少自身能量消耗而选择“分组丢失(D)”的动作；对于一个恶意传感节点,它可能选择动作“合作(C)”混淆 WSN 入侵检测代理的判断,也可能选择动作“分组丢失(D)”节省自身的数据转发能量消耗,而其最终目的是选择动作“传播(P)”尽可能多地传播恶意程序以便可以窃听更多的感知信息、阻塞数据通信甚至使用耗尽能量的方法造成传感节点彻底瘫痪。对于 WSN 入侵检测代理,可选择动作“提交($\tilde{s}$)”将监控数据提交到 IDSaaS 实现恶意程序的检测,也可以因为考虑能量消耗和隐私保护的需要选择动作“空闲(I)”不提交监控数据。

根据上述分析,传感节点和 WSN 入侵检测代理进行博弈时总共有 6 组动作对。对于“动作对”(C, $\tilde{s}$),传感节点因选择动作 C 将正常地感知信息并帮助其他节点转发感知数据,这对整个 WSN 有利,因此给予合作收益(记为 φ_C),同时负担感知信息和数据转发等合作成本(记为 x_C),还因为 WSN 入侵检测代理选择动作 $\tilde{s}$ 导致传感节点的隐私泄露(记为 $x_{\tilde{p}}$),所以此时传感节点的总支付(记为 o_{CS}^x , $x \in \Phi_i$)为:

$$\forall x \in \Phi_i, o_{CS}^x = \varphi_C - x_C - x_{\tilde{p}} \quad (1)$$

WSN 入侵检测代理因选择动作 Ξ 将监控数据提交到 IDSaaS,这样会产生提交监控数据时的能量消耗以及调用 IDSaaS 的成本(记为 $x_{\tilde{s}}$),另外由于任何的入侵检测系统具有误报率(记为 γ),从而可能将一个正常的合作行为误判为恶意

的传播行为,导致误报损失 $\gamma\omega$,其中 ω 表示一次误报导致的损失,所以此时 WSN 入侵检测代理的总支付(记为 o_{CS}^j)为:

$$o_{CS}^j = -x_{\tilde{s}} - \gamma\omega \quad (2)$$

对于“动作对”(C, I),传感节点将得到合作收益 φ_C 并负担合作成本 x_C ,但因 WSN 入侵检测代理选择动作 I 不会泄露传感节点的隐私,所以此时传感节点的总支付(记为 o_{CI}^x , $x \in \Phi_i$)为:

$$\forall x \in \Phi_i, o_{CI}^x = \varphi_C - x_C \quad (3)$$

WSN 入侵检测代理选择动作 I 不会得到收益也不会产生成本,所以此时的总支付为 0。对于“动作对”(D, $\tilde{s}$),传感节点因采取动作 D 不会得到收益也不会产生成本,而 WSN 入侵检测代理选择动作 Ξ 将产生提交监控数据时的能量消耗以及调用 IDSaaS 的成本,所以此时它们的总支付分别为 0 和 $-x_{\tilde{s}}$ 。

对于“动作对”(D, I),显然传感节点和 WSN 入侵检测代理的总支付都为 0。对于“动作对”(P, $\tilde{s}$),恶意传感节点若传播成功恶意程序且未被 IDSaaS 成功检测,则得到收益 $(1-\eta)\lambda\varphi_p$,其中 η 表示 IDSaaS 的检测率, λ 表示恶意程序传播成功率, φ_p 表示恶意程序传播得到的收益。同时它将承担因传播恶意程序产生的成本(记为 x_p)以及隐私泄露 $x_{\tilde{p}}$ 。另外,它还将承担因 IDSaaS 成功检测恶意程序造成的损失 $\rho\eta\varphi_{\tilde{s}}$,其中 ρ 表示为反映 WSN 数据传输不可靠性而引入的监控数据成功获取概率, $\varphi_{\tilde{s}}$ 表示 IDSaaS 检测恶意程序得到的收益;所以,此时传感节点的总支付(记为 o_{PS}^x , $x \in \{\phi_i^M\}$)为:

$$\forall x \in \{\phi_i^M\}, o_{PS}^x = (1-\eta)\lambda\varphi_p - x_p - \rho\eta\varphi_{\tilde{s}} \quad (4)$$

WSN 入侵检测代理因选择动作 $\tilde{s}$ 将得到成功检测恶意程序的收益 $\rho\eta\varphi_{\tilde{s}}$,同时承担未能检测到恶意程序传播的损失 $(1-\eta)\lambda\varphi_p$ 和提交监控数据时的能量消耗以及调用 IDSaaS 成本 $x_{\tilde{s}}$,所以此时 WSN 入侵检测代理的总支付(记为 o_{PS}^j)为:



$$o_{PS}^j = \rho\eta\varphi_S - (1-\eta)\lambda\varphi_P - x_{\bar{S}} \quad (5)$$

对于“动作对” (P, I) ，恶意传感节点将得到恶意程序传播收益 $\lambda\varphi_P$ ，同时承担恶意程序传播成本 x_P ，所以，此时传感节点的总支付（记为 o_{PI}^x ， $x \in \{\phi_i^M\}$ ）为：

$$\forall x \in \{\phi_i^M\}, o_{PI}^x = \lambda\varphi_P - x_P \quad (6)$$

WSN 入侵检测代理将承担恶意程序传播造成的损失，所以此时的总支付为 $-\lambda\varphi_P$ 。综上可得，传感节点和 WSN 入侵检测代理进行博弈的支付矩阵，见表 1。

实际上，传感节点和 WSN 入侵检测代理之间的博弈是重复进行的，为了计算时刻 t （ $t \in Z^+$ ）抑制恶意程序传播的优化策略，需要事先得到一个传感节点在时刻 t 属于传感节点类型 ϕ_i^N 、 ϕ_i^S 、 ϕ_i^M 的概率，即定义 1 中集合 Ψ 的元素 $p_t(\phi_i^N)$ 、 $p_t(\phi_i^S)$ 、 $p_t(\phi_i^M)$ 。当 $t=1$ 时， $p_t(\phi_i^S)$ 和 $p_t(\phi_i^M)$ 值一般由安全专家估计得到，并在此基础上计算 $1-p_1(\phi_i^S)-p_1(\phi_i^M)$ 得到 $p_1(\phi_i^N)$ ；而当 $t \geq 1$ 时， $p_{t+1}(\phi_i^N)$ 、 $p_{t+1}(\phi_i^S)$ 、 $p_{t+1}(\phi_i^M)$ 元素值的计算需要根据恶意传感节点传播恶意程序的概率、IDSaaS 的检测率和误报率、监控数据成功获取概率等因素来决定，下面利用贝叶斯法则给出相应的计算方法。

定义 2 对 $\forall \phi \in \Phi_i$ 、 $\forall a \in A_i(\phi)$ ，记 $P_t(a|\phi)$ 表示在时刻 t 类型为 ϕ 的传感节点选择动作 a 的条件概率，则一个传感节点在时刻 t （ $t \in Z^+$ ）属于传感节点类型 ϕ 的概率 $P_{t+1}(\phi)$ 为：

$$P_{t+1}(\phi) = \frac{P_t(\phi) \cdot p_t(a|\phi)}{\sum_{\tilde{\phi} \in \Phi_i} P_t(\tilde{\phi}) \cdot p_t(a|\tilde{\phi})} \quad (7)$$

并且满足：

$$P_t(\phi_i^N) + P_t(\phi_i^S) + P_t(\phi_i^M) = 1 \quad (8)$$

$$P_t(C|\phi_i^S) = \rho(1-\gamma) \quad (9)$$

$$P_t(D|\phi_i^N) = 1-\rho \quad (10)$$

$$P_t(P|\phi_i^N) = \rho\gamma \quad (11)$$

$$P_t(C|\phi_i^S) = \eta(1-\gamma) \quad (12)$$

$$P_t(D|\phi_i^S) = 1-\eta \quad (13)$$

$$P_t(P|\phi_i^S) = \eta\gamma \quad (14)$$

$$P_t(C|\phi_i^M) = \rho(1-\gamma)(1-\alpha_i^*) \quad (15)$$

$$P_t(D|\phi_i^M) = 1-\rho \quad (16)$$

$$P_t(P|\phi_i^M) = \rho(\alpha_i^* + (1-\alpha_i^*)\gamma) \quad (17)$$

式(15)和式(17)中， α_i^* 表示在时刻 t 恶意传感节点选择动作 P 的优化概率，该值通过计算 WSN 恶意程序传播抑制博弈的精炼贝叶斯均衡得到。

4 基于精炼贝叶斯均衡抑制 WSN 恶意程序传播的优化方法

定义 1 给出的 WSN 恶意程序传播抑制博弈属于动态贝叶斯博弈类型，对应的均衡概念称为“精炼贝叶斯均衡”，其最大的特点是参与者在重复博弈过程中根据贝叶斯法则可以不断修正其他参与者类型的概率（如定义 2 给出了传感节点类型概率修正公式），并根据修正后的概率（后验概率）

表 1 传感节点和 WSN 入侵检测代理进行博弈的支付矩阵

		提交 ($\bar{S}$)	空闲 (I)
传感节点属于正常节点	合作 (C)	$\varphi_C - x_C - x_P, -x_{\bar{S}} - \gamma\omega$	$\varphi_C - x_C, 0$
传感节点属于自私节点	合作 (C)	$\varphi_C - x_C - x_P, -x_{\bar{S}} - \gamma\omega$	$\varphi_C - x_C, 0$
	分组丢失 (D)	$0, -x_{\bar{S}}$	$0, 0$
传感节点属于恶意节点	合作 (C)	$\varphi_C - x_C - x_P, -x_{\bar{S}} - \gamma\omega$	$\varphi_C - x_C, 0$
	分组丢失 (D)	$0, -x_{\bar{S}}$	$0, 0$
	传播 (P)	$(1-\eta)\lambda\varphi_P - x_P - x_{\bar{P}} - \rho\eta\varphi_S, \rho\eta\varphi_S - (1-\eta)\lambda\varphi_P - x_{\bar{S}}$	$\lambda\varphi_P - x_P, \lambda\varphi_P$

选择优化策略。

定理 1 WSN 恶意程序传播抑制博弈模型 Ξ 在时刻 t 存在混合策略精炼贝叶斯均衡。

证明: 记 α_t 和 δ_t 分别为恶意传感节点和 WSN 入侵检测代理在时刻 t 选择动作 P 和 $\tilde{S}$ 的概率。对 WSN 入侵检测代理而言, 在时刻 t 选择动作 $\tilde{S}$ 和 I 的期望收益 $\mu_t^{j,\tilde{S}}$ 和 $\mu_t^{j,I}$ 分别为:

$$\begin{aligned} \mu_t^{j,\tilde{S}} = & (1 - p_t(\phi_t^S) - p_t(\phi_t^M))(-x_{\tilde{S}} - \gamma\omega) + \\ & p_t(\phi_t^S)(-x_{\tilde{S}}) + \\ & p_t(\phi_t^M)(1 - \alpha_t)(-x_{\tilde{S}} - \gamma\omega) + \\ & p_t(\phi_t^M)(1 - \rho)(-x_{\tilde{S}}) + \\ & p_t(\phi_t^M)\alpha_t(\rho\eta\phi_{\tilde{S}} - (1 - \eta)\lambda\phi_p - x_{\tilde{S}}) \end{aligned} \quad (18)$$

$$\mu_t^{j,I} = p_t(\phi_t^M)\alpha_t(-\lambda\phi_p) \quad (19)$$

再由达到精炼贝叶斯均衡时 WSN 入侵检测代理选择动作 $\tilde{S}$ 和 I 的不相关性可得:

$$\mu_t^{j,\tilde{S}} = \mu_t^{j,I} \quad (20)$$

从而可得到恶意传感节点在时刻 t 选择动作 p 的优化策略 α_t^* 为:

$$\alpha_t^* = \frac{x_{\tilde{S}} + \gamma\omega - p_t(\phi_t^S) + p_t(\phi_t^M)x_{\tilde{S}} - p_t(\phi_t^M)\rho x_{\tilde{S}}}{p_t(\phi_t^M)(\gamma\omega + \rho\eta\phi_{\tilde{S}} + \eta\lambda\phi_p)} \quad (21)$$

对恶意传感节点而言, 在时刻 t 选择动作 C 和 P 的期望收益 $\mu_t^{i,C}$ 和 $\mu_t^{i,P}$ 分别为:

$$\begin{aligned} \mu_t^{i,C} = & (1 - p_t(\phi_t^S) - p_t(\phi_t^M))(\delta_t(\phi_C - x_C - x_{\tilde{P}}) + \\ & (1 - \delta_t)(\phi_C - x_C) + p_t(\phi_t^S)(\delta_t(\phi_C - x_C - x_{\tilde{P}}) + \\ & (1 - \delta_t)(\phi_C - x_C) + p_t(\phi_t^M)(\delta_t(\phi_C - x_C - x_{\tilde{P}}) + \\ & (1 - \delta_t)(\phi_C - x_C) \end{aligned} \quad (22)$$

$$\mu_t^{i,P} = p_t(\phi_t^M)\delta_t((1 - \eta)\lambda\phi_p - x_p - x_{\tilde{P}} - \rho\eta\phi_{\tilde{S}}) + (1 - \delta_t)(\lambda\phi_p - x_p) \quad (23)$$

再由达到精炼贝叶斯均衡时恶意传感节点选择动作 C 和 P 的不相关性可得:

$$\mu_t^{i,C} = \mu_t^{i,P} \quad (24)$$

从而可得到 WSN 入侵检测代理在时刻 t 选择动作 $\tilde{S}$ 的优化策略 δ_t^* 为:

$$\delta_t^* = \frac{\phi_C - x_C - p_t(\phi_t^M)(x_p - \lambda\phi_p)}{x_{\tilde{P}} - p_t(\phi_t^M)(\eta\lambda\phi_p + x_{\tilde{P}} + \rho\eta\phi_{\tilde{S}})} \quad (25)$$

综上所述, WSN 恶意程序传播抑制博弈模型 Ξ 在时刻 t 存在混合策略精炼贝叶斯均衡, 即: 恶意传感节点在时刻 t 以概率 α_t^* 选择动作 P , 而 WSN 入侵检测代理在时刻 t 以概率 δ_t^* 选择动作 $\tilde{S}$ 。也就是说, 当 WSN 入侵检测代理在时刻 t 以概率 δ_t^* 选择动作 $\tilde{S}$ 时, 将达到最大化抑制 WSN 恶意程序传播的目的。证毕。

在实际运用定理 1 得到的结果时, 首先由管理员设置 WSN 入侵检测代理的动作为 I , 再依据定义 1 设置 WSN 恶意程序传播抑制博弈模型的博弈参数, 然后依据表 1 初始化博弈模型的支付矩阵, 一旦 WSN 入侵检测代理监测到传感节点发出的行为数据后, 将依据式 (25) 计算优化的提交策略, 由得到的优化策略决定是否将监控数据发送到 IDSaaS, 然后 IDSaaS 依据检测结果返回针对传感节点的控制信息, 实现最大化抑制 WSN 恶意程序传播的目的。下面给出具体的算法。

算法 1 基于精炼贝叶斯均衡抑制 WSN 恶意程序传播的算法

```

 $t \leftarrow 1$ ;
设置博弈参数  $\gamma$ 、 $\omega$ 、 $\eta$ 、 $\lambda$ 、 $\rho$ 、 $\phi_C$ 、 $\phi_P$ 、 $\phi_{\tilde{S}}$ 、 $x_C$ 、 $x_{\tilde{P}}$ 、 $x_{\tilde{S}}$ 、 $x_p$ 、 $p_1(\phi_1^S)$ 、 $p_1(\phi_1^M)$ ;
设置 WSN 入侵检测代理的动作为  $I$ ;
do until 博弈结束;
if WSN 入侵检测代理监测到监控数据;
if 存在 WSN 恶意程序传播抑制博弈模型;
    获取存储的 WSN 恶意程序传播抑制博弈模型;
else;
    依据定义 1 构建 WSN 恶意程序传播抑制博弈模型;
end if;
依据式 (25) 计算  $\delta_t^*$ ;
依据  $\delta_t^*$  选择动作  $\tilde{S}$ ;
依据式 (7) 计算  $p_{t+1}(\phi_t^S)$  和  $p_{t+1}(\phi_t^M)$ ;

```



$$p_t(\phi_i^S) \leftarrow p_{t+1}(\phi_i^S);$$

$$p_t(\phi_i^M) \leftarrow p_{t+1}(\phi_i^M);$$

$$t \leftarrow t+1;$$

end do

5 实验分析

通过 MATLAB 实验工具计算 WSN 入侵检测代理在时刻 t 选择动作 $\tilde{S}$ 的优化策略 δ_t^* ，比较其中的影响因素，从而为实际应用提供实验依据。考虑 WSN 实际情况，实验参数设置如下： $\delta_C = 50$ ， $\delta_p = 100$ ， $\delta_s = 50$ ， $x_p = 30$ ， $x_p = 20$ ， $x_C = 40$ ， $p_t(\phi_i^S) = p_t(\phi_i^M) = 0.3333$ 。值得注意的是，虽然这些参数设置了选定的值，但合理改变这些参数值时能得到类似的实验结果变化趋势。

图 2 给出了当监控数据成功获取概率 ρ 值固定，而恶意程序传播成功率 λ 和 IDSaaS 检测率 η 值动态变化时，WSN 入侵检测代理在时刻 t 选择动作 $\tilde{S}$ 的优化策略 δ_t^* 的变化情况。

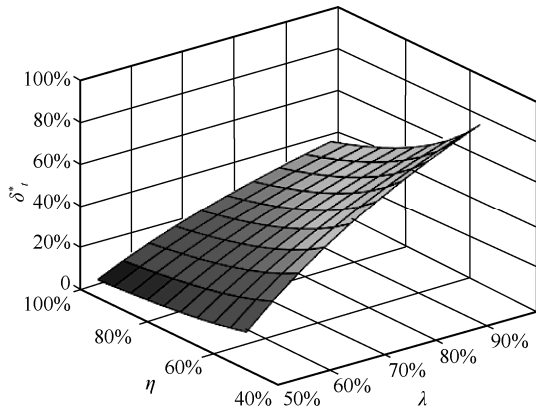


图 2 考虑 λ 和 η 因素变化时 δ_t^* 的变化趋势

从图 2 中可以看出， δ_t^* 值随着 λ 值的增大而增大，但随着 η 值的增大而减小。并且 λ 值的变化对 δ_t^* 值的变化影响更大。例如，当 $\eta = 0.8$ 并且 λ 值从 0.5 变化到 0.95 时， δ_t^* 值从约 0.1154 变化到约 0.5198，增长了约 350.43%；而当 $\lambda = 0.8$ 并且 η 值从 0.5 变化到 0.95 时， δ_t^* 值从约 0.6977 变化到约 0.3517，

减少了约 49.59%。

图 3 给出了当恶意程序传播成功率 λ 值固定，而 IDSaaS 检测率 η 和监控数据成功获取概率 ρ 值动态变化时，WSN 入侵检测代理在时刻 t 选择动作 $\tilde{S}$ 的优化策略 δ_t^* 的变化情况。从图 3 中可以看出， δ_t^* 都随着 η 和 ρ 值的增大而减小。并且 η 值的变化对 δ_t^* 值的变化影响更大。

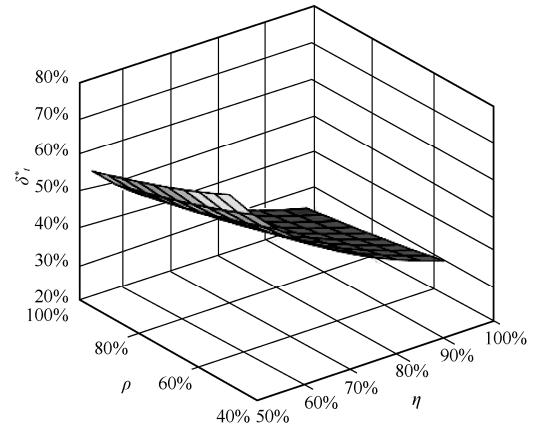


图 3 考虑 η 和 ρ 因素变化时 δ_t^* 的变化趋势

图 4 给出了当 IDSaaS 检测率 η 值固定，而恶意程序传播成功率 λ 和监控数据成功获取概率 ρ 值动态变化时，WSN 入侵检测代理在时刻 t 选择动作 $\tilde{S}$ 的优化策略 δ_t^* 的变化情况。从图 4 中可以看出， λ 值的变化对 δ_t^* 值的变化影响更大。

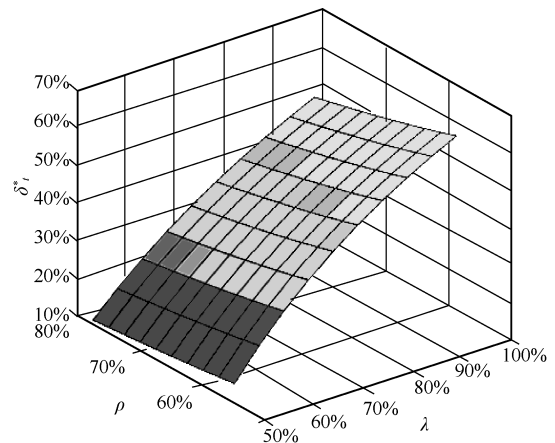


图 4 考虑 λ 和 ρ 因素变化时 δ_t^* 的变化趋势

综合上述的实验结果变化趋势，对 WSN 入侵检测代理在时刻 t 选择动作 $\tilde{S}$ 的优化策略 δ_t^* 影响

最大的是 λ ，其次是 η ，最后是 ρ 。这与WSN恶意程序传播实际情况相一致，当恶意程序传播成功率 λ 增大时，WSN入侵检测代理将显著增大 δ_i^* 值，从而最大化地抑制WSN恶意程序的传播。另外，提高IDSaaS检测率比提高监控数据成功获取概率能更好地抑制WSN恶意程序的传播，这对于实际系统研发具有指导意义。

6 结束语

借助云计算和动态贝叶斯博弈，本文提出了一种有效应用入侵检测系统检测WSN恶意程序从而抑制WSN恶意程序传播的方法。基于云计算的WSN入侵检测网络结构考虑WSN节点资源有限和云计算平台资源几乎无限的现状，解决了WSN入侵检测代理部署和入侵检测计算资源消耗大的问题。基于动态贝叶斯博弈建立的WSN恶意程序传播抑制博弈模型，反映了WSN入侵检测代理监控数据发送能耗和传感节点隐私保护需求，解决了在考虑传感节点隐私保护前提下最大化抑制WSN恶意程序传播的决策问题，给出的算法为具体应用提供了思路。实验结果给出了抑制WSN恶意程序传播优化策略的影响因素，对实际系统研发具有指导意义。

本文基于云计算的WSN入侵检测网络结构提高了检测结果的准确度，解决了WSN入侵检测资源消耗大的问题，但是，这种体系结构同时增加了网络数据时延和通信负载，未来工作将考虑采用云计算和边缘计算相结合的WSN入侵检测网络结构来解决上述问题。

参考文献:

- [1] 罗军舟, 杨明, 凌振, 等. 网络空间安全体系与关键技术[J]. 中国科学: 信息科学, 2016, 46(8): 939-968.
LUO J Z, YANG M, LING Z, et al. Architecture and key technologies of cyberspace security[J]. Scientia Sinica: Informationis, 2016, 46(8): 939-968.
- [2] 张焕国, 韩文报, 来学嘉, 等. 网络空间安全综述[J]. 中国科学: 信息科学, 2016, 46(2): 125-164.
ZHANG H G, HAN W B, LAI X J, et al. Survey on cyberspace security[J]. Scientia Sinica: Informationis, 2016, 46(2): 125-164.
- [3] 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.
- [4] 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 meets wireless sensor networks security[M]. Beijing: Tsinghua University Press, 2016.
- [5] 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.
- [6] 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.
- [7] 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.
- [8] ILLIANO V P, LUPU E C. Detecting malicious data injections in wireless sensor networks: a survey[J]. ACM Computing Surveys, 2015, 48(2): 33.
- [9] YANG Y, ZHU S, CAO G. Improving sensor network immunity under worm attacks: a software diversity approach[J]. Ad Hoc Networks, 2016, (47): 26-40.
- [10] GHOSAL A, HALDER S. A survey on energy efficient intrusion detection in wireless sensor networks[J]. Journal of Ambient Intelligence and Smart Environments, 2017, 9(2): 239-261.
- [11] ZARPELÃO B B, MIANI R S, KAWAKANI C T, et al. A survey of intrusion detection in Internet of things[J]. Journal of Network and Computer Applications, 2017(84): 25-37.
- [12] 曹旭, 曹瑞彤. 基于大数据分析的网络异常检测方法[J]. 电信科学, 2014, 30(6): 152-156.
CAO X, CAO R T. Network anomaly prediction method based on big data[J]. Telecommunications Science, 2014, 30(6): 152-156.
- [13] 柳毅, 洪俊斌. 基于网络爬虫与页面代码行为的XSS漏洞动态检测方法[J]. 电信科学, 2016, 32(3): 87-91.
LIU Y, HONG J B. A dynamic detection method based on Web crawler and page code behavior for XSS vulnerability[J]. Tele-



- communications Science, 2016, 32(3): 87-91.
- [14] 李传煌, 孙正君, 袁小雍, 等. 基于深度学习的实时 DDoS 攻击检测[J]. 电信科学, 2017, 33(7): 53-65.
LI C H, SUN Z J, YUAN X Y, et al. Real-time DDoS attack detection based on deep learning[J]. Telecommunications Science, 2017, 33(7): 53-65.
- [15] 汪来富, 金华敏, 刘东鑫, 等. 面向网络大数据的安全分析技术应用[J]. 电信科学, 2017, 33(3): 112-118.
WANG L F, JIN H M, LIU D X, et al. Application of security analysis technology for network big data[J]. Telecommunications Science, 2017, 33(3): 112-118.
- [16] 刘建华, 李明禄, 李立志, 等. 工业无线传感云中面向移动机器人的自适应信任演化机制[J]. 电信科学, 2017, 33(6): 86-96.
LIU J H, LI M L, LI D Z, et al. Adaptation trust evolution scheme for mobile robot in industrial wireless sensor-cloud[J]. Telecommunications Science, 2017, 33(6): 86-96.
- [17] IQBAL S, MAT KIAH M L, DHAGHIGHI B, et al. On cloud security attacks: a taxonomy and intrusion detection and prevention as a service[J]. Journal of Network and Computer Applications, 2016(74): 98-120.
- [18] SUN H, WANG X, BUYYA R, et al. CloudEyes: cloud-based malware detection with reversible sketch for resource-constrained internet of things (IoT) devices[J]. Software-Practice and Experience, 2017, 47(3): 421-441.
- [19] 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, 43(1): 144-150.
WANG J D, YU D K, ZHANG H W, et al. Active defense strategy selection based on the static Bayesian game[J]. Journal of Xidian University, 2016, 43(1): 144-150.
- [20] 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, 23(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, 23(3): 712-723.
- [21] 沈士根, 黄龙军, 胡珂立, 等. 基于微分博弈的在线社交网络恶意程序传播优化控制方法[J]. 电信科学, 2015, 31(10): 66-73.
SHEN S G, HUANG L J, HU K L, et al. Differential game-based optimal control method for preventing malware propagation in online social network[J]. Telecommunications Science, 2015, 31(10): 66-73.
- [22] 张恒巍, 李涛. 基于多阶段攻防信号博弈的最优主动防御[J]. 电子学报, 2017, 45(2): 431-439.
ZHANG H W, LI T. Optimal active defense based on multi-stage attack-defense signaling game[J]. Acta Electronica Sinica, 2017, 45(2): 431-439.
- [23] 黄健明, 张恒巍, 王晋东, 等. 基于攻防演化博弈模型的防御策略选取方法[J]. 通信学报, 2017, 38(1): 168-176.
HUANG J M, ZHANG H W, WANG J D, et al. Defense strategies selection based on attack-defense evolutionary game model[J]. Journal of Communications, 2017, 38(1): 168-176.
- [24] SPYRIDOPOULOS T, MARASLIS K, MYLONAS A, et al. A game theoretical method for cost-benefit analysis of malware dissemination prevention[J]. Information Security Journal, 2015, 24(4-6): 164-176.
- [25] YUAN Y, SUN F, LIU H. Resilient control of cyber-physical systems against intelligent attacker: a hierarchical stackelberg game approach[J]. International Journal of Systems Science, 2016, 47(9): 2067-2077.
- [26] 周恒杰, 孙闽红, 钟华, 等. 基于不完全信息动态博弈的多信道无线网络抗干扰传输[J]. 电信科学, 2018, 34(2): 39-45.
ZHOU H J, SUN M H, ZHONG H, et al. Anti-jamming transmission in a multi-channel wireless network based on incomplete information dynamic game[J]. Telecommunications Science, 2018, 34(2): 39-45.
- [27] WANG K, DU M, YANG D, et al. Game-theory-based active defense for intrusion detection in cyber-physical embedded systems[J]. ACM Transactions on Embedded Computing Systems, 2016, 16(1): 18-21.
- [28] NAUMAN M, AZAM N, YAO J. A three-way decision making approach to malware analysis using probabilistic rough sets[J]. Information Sciences, 2016(374): 193-209.
- [29] HAYEL Y, ZHU Q. Epidemic protection over heterogeneous networks using evolutionary poisson games[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(8): 1786-1800.

[作者简介]



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。



冯晟 (1979-), 男, 博士, 绍兴文理学院计算机科学与工程系讲师, 主要研究方向为无线传感器网络、物联网、计算机视觉、智能机器人。

黄龙军 (1976-), 男, 博士, 绍兴文理学院计算机科学与工程系讲师, 主要研究方向为无线传感器网络、博弈论。

胡珂立 (1989-), 男, 博士, 绍兴文理学院计算机科学与工程系讲师, 主要研究方向为图像处理、目标跟踪、中智理论。

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。