WSN 中一种新的基于重复博弈的入侵检测研究*

刘雅菲，刘宴兵
（重庆邮电大学 计算机科学与技术学院，重庆 400065）

摘　要：当物联网中存在攻击节点时，目前的研究方法对其无约束作用。为了解决这一问题，提出了一种带惩罚机制的基于重复博弈的入侵检测模型。首先分析节点的本次攻击行为对后续收益的影响，在此基础上建立了一种惩罚机制，通过这种机制，节点选择攻击的概率将大大降低；其次结合模型分析了节点对将来利益的重视程度，以及入侵检测率对结果的影响。仿真结果表明，当网络中存在攻击节点时，该模型能有效遏制节点攻击。

关键词：物联网；无线传感网；入侵检测；重复博弈
中图分类号：TN915.08　　**文献标志码：**A　　**文章编号：**1001-3695(2013)05-1540-04
doi:10.3969/j.issn.1001-3695.2013.05.067

Novel research of intrusion detection based on repeated game in wireless sensor network

LIU Ya-fei, LIU Yan-bing
(*College of Computer Science & Tecnology*, *Chongqing University of Posts & Telecommunications*, *Chongqing* 400065, *China*)

Abstract: When things in the presence of attack node, the current study method for unconstrained function. This paper proposes a novel intrusion detection model with punishment based on repeated game. If a malicious node attacks at this time, the act will effect it's utility at next time. Base on this, this paper gave a punish method, in this method, the probability of a node chooses attack would reduce, and analysis the future payoff expectations, the detection rate of intrusion detection. Simulation results show that, this model can effectively curb the node attack when a malicious node attacks the network.

Key words: Internet of things(IoT); wireless sensor network(WSN); intrusion detection; repeat game

0　引言

物联网(IoT)是一种建立在互联网基础上的泛在网络，它通过将各种有线和无线网络与互联网融合，应用海量的传感器、智能处理终端、全球定位系统等实现物与物、物与人、所有的物品与网络的连接，方便人们的识别、管理和控制[1]。目前，物联网相关技术已成为各国竞争的焦点和制高点，因此通过研究物联网的相关基础理论和关键技术，挑战物联网的重大基础科学问题，发展我国具有自主知识产权的物联网技术，具有十分重要国际战略意义。无线传感器网络是物联网中感知事物传输数据的重要手段，可以构成物联网的重要触角和神经。因此，无线传感器网络的研究成为了物联网中研究的重要内容。

本文针对基于重复博弈的入侵检测节点行为策略模型的研究为理论基础进行了深入分析。提出了一种新的基于重复博弈的入侵检测预测模型，通过采用适用的惩罚机制和重复博弈的贴现率来分析博弈者本轮收益对未来收益的影响，降低攻击者攻击概率，提高网络整体性能。最后通过仿真实验验证了该模型的可行性。

1　相关研究现状

无线传感器网络(WSN)是由部署在监测区域内大量的廉价微型传感器节点组成，通过无线通信的方式形成一个多跳的自组织网络系统，协作感知、采集和处理网络覆盖区域中感知对象的信息，并发送给观察者[2]。入侵检测系统(intrusion detection system, IDS)在网络安全中占据重要的地位。目前已经开发出了多种入侵检测系统，但大多数系统仍然是被动的防御技术，不能主动地分析和判断入侵事件所带来的影响。无线节点的移动性、无线信道的开放性更使得无线网络的安全性变得非常脆弱，网络使用者本能的自私行为很难受到遏制，无线节点之间的行为往往相互影响并难以集中管理，而博弈理论[3~5]正是研究无线网络安全问题的有力工具。

目前，关于入侵检测的研究主要且多数建立在一次性博弈分析的基础上[6]，而鉴于真实场景中攻击不可能是只发动一次攻击，考虑到攻击的重复性，将其视为一个重复的多阶段博弈[7]的过程显然更为合理。文献[8]建立了无线传感器网络中基于重复博弈理论的攻防模型，取得了比较理想的效果。在文献[9]中，基于重复博弈理论的基础上，对 Ad hoc 网络中相邻节点的合作转发过程建立了无限重复博弈模型，提出了一种通用惩罚机制，对节点不合作行为给予严厉惩罚，确保节点恢复到合作状态。在文献[10]中，针对 Ad hoc 网络节点转发过程，提出了一个基于本地检测及孤立惩戒机制的重复博弈转发模型，并通过建立模型提出一个激励性一致性条件，通过选择合理参数分析，能够有效抵制网络规模的增长及节点合作意

收稿日期：2012-09-12；**修回日期：**2012-10-22　**基金项目：**“新一代宽带无线移动通信网”国家科技重大专项课题(2011ZX03002-004-03)；国家教育部 NCET 项目；重庆市高等教育成果转化项目(Kjzh10206)；国家公安部信息网络安全重点实验室项目(C11609)

作者简介：刘雅菲(1987-)，女，重庆人，硕士研究生，主要研究方向为网络信息安全(474598231@qq.com)；刘宴兵(1971-)，男，四川遂宁人，教授，博士，主要研究方向为网络通信安全、网格计算.

愿,提高自私节点存在时的网络性能。

因此,本文建立的重复博弈模型是针对网络中存在攻击节点的现象时进行的分析和研究。

2　重复博弈模型

重复博弈(repeated game)[11]是指同样结构的博弈重复多次,其中的每次博弈称为阶段博弈(stage game)。重复博弈是动态博弈中的重要内容,它可以是完全信息的重复博弈,也可以是不完全信息的重复博弈。当博弈只进行一次时,每个参与人都只关心一次性的效用;如果博弈是重复多次的,参与者可能会为了长远利益而牺牲眼前的利益,从而选择不同的均衡策略。因此,重复博弈的次数将会影响到博弈均衡的结果。

本文将博弈过程视为无限重复的,这是因为节点无法预知博弈何时终止。从博弈论的观点来看,当终点无法预测时,局中人将不得不以无限重复的方式来评估当前策略及其对后继局势的影响。这一假设在转发场景中是合理的,它使得节点无法准确判断某次惩罚是否会因网络运行终止而得不到正确的实施,从而杜绝了其利用这一知识对作弊策略进行逆向推导的可能。

2.1　重复博弈模型定义

定义 1　攻击防御模型 RDM(repeated game defend model)包括四个元组(参与人,行动空间,收益函数,重复博弈次数),组元定义如下:

a)参与人。包括参与人 attacker 和防御者 IDS,i 代表 attacker,j 代表 IDS,其中参与人 i 的类型空间为 $\theta_i = \{m,r\}$,m 代表参与人的类型是恶意节点,能对网络造成一定的威胁和破坏,r 代表参与人是正常访问网络的节点,不能对网络造成破坏。参与人 j 的类型空间为 $\theta_j = \{d\}$,d 代表参与人 j 能检测和阻止其他节点的攻击。

b)行动空间。通过对以往的研究,本文综合考虑到攻击者的两种主要行动即攻击(attack)和正常(normal),记为行动空间 $A_i(\theta_i) = \{N,A\}$。同样的,IDS 有两种行动:如果没有检测到异常,则允许用户继续(continue);一旦检测到威胁时,监督 defend 用户的行动。IDS 的行动空间记为 $A_j(\theta_j) = (C,D)$。

c)收益函数。它指每个参与人在参与博弈时依据其所属类型和选择的行动可获得的收益,包括 $u_i(\theta_i)$、$u_j(\theta_j)$。

d)重复博弈次数。本文将博弈过程视为无限重复的,这是因为节点无法预知博弈何时终止,因此博弈过程重复进行 T 次,其中 $T = \infty$。

因此得到本文的攻击防御模型,用 RDM = $\{\theta_i, \theta_j; A_i(\theta_i), A_j(\theta_j); u_i(\theta_i), u_j(\theta_j); T\}$ 来表示。

2.2　阶段博弈

为方便分析,本文假定这样一种网络环境:整个网络运行的时间由一系列离散的时隙 t 构成,博弈每方的行动类型都相同,每个时隙的长度都可以保证博弈的过程。在任一时隙里都有博弈过程的进行,并且假设在每个时隙内 IDS 只能保护一个节点。在每个时隙 t 里都有数据包需要传送,如果有其中一个节点拒绝转发数据包,那么这个数据包的传输就失败,数据包发送成功的概率就为 0。

根据文献[12]提出的博弈模型,本文对模型 RDM 的各个符号作出定义,如表 1 所示。

表 1　RDM 符号定义

符号	定义
U_i	网络效用,攻击者获得效用
C_d	IDS 发动防御代价
C_i	攻击者发动攻击代价
q	IDS 入侵检测率

通过分析重复博弈模型 RDM 博弈的过程,得到阶段博弈的博弈双方收益矩阵,如表 2 所示。

表 2　RDM 博弈双方效用

attacker	IDS	
	defend	continue
attack	$(1-q)U_i - C_i, U_i - qC_d$	$U_i - C_i, 0$
normal	$0, U_i - C_d$	$0, U_i$

在本文的重复模型 RDM 中,当阶段博弈的双方采用这样的策略对时(attack,defend),简记为(A,D),博弈将趋于纳什均衡。从以上分析可以得出这样的结论:对于 IDS 来说,就是找到一个恰当的节点对其进行保护;对攻击者来说,就是找到一个最恰当的节点进行攻击,而且攻击者攻击所获得的收益总是大于不攻击时的收益,所以对于攻击者来说总是被鼓励攻击,这样的认识对接下来的讨论非常重要。

2.3　重复博弈

定义 2　在重复博弈模型 RDM 中,考虑在每轮的博弈 G_i 中,在第 t 个周期参与者 i 选取行动记为 $\bar{g}_{it}$,$\bar{g}_{it} \in G_i$,则 t 个周期的行动组合记为 $\bar{g}_t = (\bar{g}_{1t}, \bar{g}_{2t}, \cdots, \bar{g}_{nt})$,博弈者 i 的总效用就可以表示为各轮效用的贴现和。根据文献[13],给定一个贴现因子 δ,$\delta \in (0,1)$,可以被视为对利益的综合度量,δ 越大,则 i 越重视长期利益;δ 越小,则 i 越重视眼前利益。其中 $u_i(\bar{g}_{it}, \bar{g}_{-it})$ 代表节点 i 在第 t 个周期阶段效用,则参与者 i 在重复博弈周期的总效用为 $U_i(s) = \sum_{t=1}^{\infty} \delta^{t-1} u_i(\bar{g}_{it}, \bar{g}_{-it})$。

定义 3　参与者 i 在无穷周期的平均效用为 $\bar{u}_i = (1-\delta)U_i(s)$,本文着重考虑单轮效用对整个重复博弈过程的影响[14]。

在单轮博弈中,纳什均衡(A,D)是无法避免的,当博弈进行无限轮时,可以进入这样的最优解(N,C)。如果只看单轮,攻击者只考虑单次博弈的最大效用,全然不考虑本次攻击对后继行为的收益影响,将会一直选择纳什均衡(A,D)。事实上,如果 IDS 对攻击行为有惩罚,即攻击者在单轮博弈采取的 attack 行为会带来对后继收益的损失,那么攻击者将不得不考虑 IDS 的惩罚所带来的代价;而当本次攻击会给后继的惩罚代价超过攻击带来的收益时,并且超过本次攻击带来的短期获利,那么将迫使攻击者采取不攻击行为,从而 IDS 将可以不用实施监督,减少网络成本,进而达到维护整个网络正常秩序的目的。

在以往的研究中,一旦某个节点被攻击者捕获,网络就将这个节点删除,这种行为必定会对整个网络造成影响,对攻击节点的攻击无遏制作用。因此本文考虑将攻击者捕获的恶意节点通过惩罚机制教化成正常节点,于是有这样的惩罚机制:假设恶意节点 i 在时隙 t 中发起攻击,即该节点不发送接收到的数据包,它将立即被 IDS 检测发现,系统对节点 i 迅速发起策略,并且从下一个时隙 $t+1$ 开始,都将对节点 i 实施 p 个时隙的 defend,当 defend 结束后,节点 i 的攻击历史被遗忘,可以选择重新加入网络,重新转发数据包。

3　关于重复博弈参数的分析

3.1　贴现值的影响

结论　当 δ 满足条件 $\varepsilon<\delta<1$，$\varepsilon\in(0,1)$ 属于一个常值，重复博弈的策略组合(A,D)总是一个子博弈完美纳什均衡。

证明　假设在第 t 个阶段，攻击者 attacker 出现了一次性偏离，偏离在该轮能带来的最大效用是 e_i，偏离将引发 t 轮之后 IDS 回归到单轮博弈下的纳什均衡策略 defend，当攻击者恢复原策略 attack 时，因为 IDS 偏离能够带给攻击者最大效用的策略，因此攻击者又执行策略 attack，所以第 t 轮的偏离能够带来的最大总效用是 V_i：$V_i=u_i+e_i\times\delta/(1-\delta)$。

如果 attacker 不偏离策略组合，效用始终是 u_j，从 t 阶段开始的后续子博弈能给博弈者 i 带来的效用是 $V_j=\sum_{r=t}^{\infty}\delta^{r-t}u_j=u_j/(1-\delta)$，要使选择 attack 是最优的，当 $V_i\geqslant V_j$ 时，即 $u_i+e_i\times\delta/(1-\delta)\geqslant u_j/(1-\delta)$ 时，解得当 $\delta\geqslant(u_i-u_j)/(u_i-e_i)$ 时，attacker 选择 attack、IDS 选择 defend 的策略组合就成为子博弈完美纳什均衡。

3.2　入侵检测率的影响

在上文中都是假设 IDS 检测到攻击的概率为 1，这是理想化的。考虑到实际场合中检测协议的不完美性，因此在 RDM 中假设 IDS 系统对攻击者的检测率小于 1 显然更为合理。

设 IDS 的检测率为 $q\in(0,1)$，则节点 i 攻击 k 次才被发现的概率为 $(1-q)^{k-1}q$，节点攻击的收益现值为 $A=\sum_{t=0}^{k-1}\delta^t(U_i-C_i)$，节点再次回到正常状态的收益为 $B=\delta^{p+k}\sum_{t=0}^{\infty}\delta^tC_w$，$C_w$ 是节点再次回到正常状态的效用，惩罚期间的收益为 $C=\delta^k\sum_{t=0}^{p-1}\delta^tP_c$，$P_c$ 是惩罚期间的收益，因此采取这个惩罚博弈过程节点 i 获得的预期收益现值总期望表述为

$$S_i=\sum_{k=1}^{\infty}q(1-q)^{k-1}(A+B+C)$$

解出 S_i 得

$$S_i=\frac{(1-\delta)(U_i-C_i)+q\delta(1-\delta^p)C_w+q\delta^{p+1}P_c}{(1-\delta)(1-\delta+q\delta)}\tag{1}$$

然后得到平均期望

$$\overline{S_i}=\frac{(1-\delta)(U_i-C_i)+q\delta(1-\delta^p)C_w+q\delta^{p+1}P_c}{1-\delta+q\delta}\tag{2}$$

接下来得到节点有惩罚时的效用与攻击没有惩罚时的效用差值

$$\Delta U_i=\overline{S_i}-A=\frac{q\delta(1-\delta^p)C_w+q\delta^{p+1}P_c-q\delta(U_i-C_i)}{1-\delta+q\delta}\tag{3}$$

对式(3)求 q 的偏导数非正，因此随着入侵检测率 q 的提高，节点因为攻击得到的收益减小，节点的攻击行为也越不利，节点将不选择攻击，数据包发送成功率也将提高。

当 $q=0$ 时，$\Delta U_i=0$，整个博弈将退化成单阶段博弈，这也与实际情况相符，数据包发送成功率只与单次博弈结果有关。

当 $\delta\to1$，$\Delta U_i\to P_c-(U_i-C_i)$，说明不论检测率为多少，节点都非常重视惩罚。因此节点将非常重视长远收益，节点发送数据包的成功率也就越高，这也符合直观感受。

4　实验仿真

4.1　QRE 分析

McKelvey 等人[15]对标准型博弈和扩展性博弈定义了 QRE(quantal response equilibrium)理论，以这种均衡作为一种概率型的方法来模拟博弈模型。QRE 理论同 logit 函数类似，可以作为解释参与者偏离均衡的一种方法，是纳什均衡的一种一般化表示。

Gambit 工具提供了对于广泛博弈和策略博弈的计算 logit QRE 均衡的方法。使用 Gambit 工具分析，结果如图 1 所示。

通过图 1 可以得到，在仿真开始阶段，博弈双方各自选择两种策略的概率均为 0.33，表示博弈双方几乎无法辨别各自策略优劣。随着博弈次数 λ 的增加，攻击者选择攻击的概率较快上升，选择不攻击的概率下降，同时，IDS 选择 defend 概率也随着上升，在 λ 达到 1.1 时，向纳什均衡逼近，当 λ 增加到 6.0 时，QRE 与子博弈纳什均衡一致。通过以上分析得到，随着时间的推移，重复博弈的进行，博弈双方选择的 logit QRE 均衡收敛于纳什均衡。

4.2　参数影响

仿真实验环境本文采用的是 MATLAB，场景布置在 500 m × 500 m 的区域面积内，随机放置 30 个节点，恶意节点 5 个，着重考察本文提出的模型对整个网络的影响，因此在仿真环境中着重考察传送包率，如果某一个节点被认定为恶意节点，那么其策略选择全部不转发接收到的数据包。

根据仿真结果得到在重复博弈模型下，数据包发送成功率，如图 2 所示。

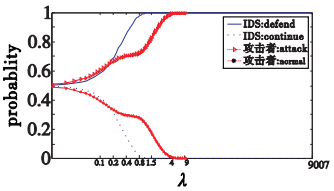

图1　Gambit实验结果

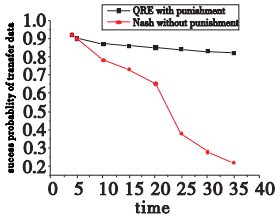

图2　数据包发送成功率对比

从图 2 可以看出，随着时间的进行、博弈次数的增加，纳什均衡防御模型的数据包发送成功率在持续下降，而本文提出的新的 RDM 模型中关于 QRE 均衡保持在比较稳定的水平。

图 3 显示了攻击节点的平均效用。为方便考察，假设系统入侵检测率 $q=1$。假设在重复博弈阶段，节点 a 在第 7 个时隙被攻击者捕获并表现出攻击，通过分析节点 a 的平均效用看到，节点在攻击时的效用远远高于节点不攻击时的效用，然后根据节点间的博弈，检测出这个攻击节点，然后从第 8 个时隙对节点 a 实施 6 个时隙的惩罚。从图 3 可以看出，实施惩罚机制后，节点 a 的效用明显下降，网络正常，没有攻击时节点的平均收益要大于本文模型中的攻击存在时的平均收益。

在以上实验中考虑的是入侵检测率为理想化的情况即 $q=1$，这显然不现实，接下来考虑在不同的检测率下，数据包发送成功的概率的变化，如图 4 所示。

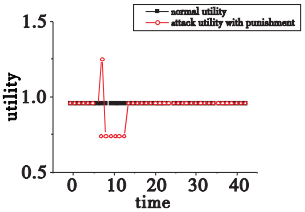

图3　攻击节点平均效用

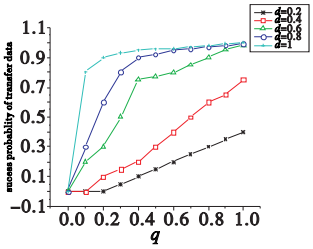

图4　入侵检测率对数据包发送成功率的影响

从图 4 可以看出，随着检测率的提高，节点发送数据包成功的概率随着节点耐心地增长得到提高，这与前文提到的式

(3)符合。这表明,随着节点对将来利益的重视程度,数据包的成功发送概率也在提高,并且在相同的 δ 下,检测率越高,数据包发送的成功概率也越高。

5　结束语

本文借鉴博弈论的思想,提出了基于无线传感网的重复博弈模型。利用重复博弈论中贴现值对模型进行分析,得出节点攻击与否对未来收益的影响。通过分析模型中节点与 IDS 的重复博弈过程,可以有效地检测出攻击节点并对其进行惩罚。实验中,首先运用博弈论工具 Gambit 验证了模型的可行性,使用 MATLAB 分析了在无线传感网中本文提出的模型,分析各个参数得到实验图。理论分析及实验结果验证了模型的可行性。下一步的工作将会深入研究入侵检测率对本文模型的影响。由于制定基于重复博弈的惩罚策略可以有效地权衡检测率和网络资源,在进一步的研究中,将通过构建真实无线传感网的条件来验证所提方案的各项性能,降低人为干预,提高系统适应能力。

参考文献:

[1] 林闯. 物联网关键理论与技术:专题前言[J]. 计算机学报,2011,34(5):761-762.

[2] AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, *et al*. Wireless sensor networks: a survey[J]. Computer Networks,2002,38(4):393-422.

[3] SHEN Shi-gen, YUE Guang-xue, CAO Qi-ying. A survey of game theory in wireless sensor networks security[J]. Journal of Networks,2011,6(3):521-532.

[4] JADIDOLESLAMY H. A high-level architecture for intrusion detection on heterogeneous wireless sensor networks: hierarchical, scalable and dynamic reconfigurable[J]. Wireless Sensor Network. 2011,3(7):241-261.

[5] KRONTIRIS I, BENENSON Z, GIANNETSOS T, *et al*. Cooperative intrusion detection in wireless sensor networks[C]//Proc of the 6th European Conference on Wireless Sensor Networks. Berlin: Springer-Verlag,2009:263-278.

[6] REDDY Y B. A game theory approach to detect malicious nodes in wireless sensor networks[C]//Proc of the 3rd International Conference on Sensor Technologies and Application. Washington DC: IEEE Computer Society,2009:462-468.

[7] SHEN Shi-gen, LI Yuan-jie, XU Hong-yun. Signaling game based strategy of intrusion detection in wireless sensor networks[J]. Computers & Mathematics with Applications, 2011, 62(6): 2404-2416.

[8] AGAH A, DAD S K. Preventing DoS attacks in wireless sensor networks: a repeated game theory approach[J]. International Journal of Network Security,2007,5(2):145-153.

[9] 王博,黄传河,杨文忠,等. Ad hoc 网络中基于惩罚机制的激励合作转发模型[J]. 计算机研究与发展, 2011,48(3):398-406.

[10] 陆音,石进,谢立. 基于重复博弈的无线自组网络协作增强模型[J]. 软件学报,2008,19(3):755-768.

[11] MANSHAEI M H, ZHU Quan-yan, ALPCAN T, *et al*. Game theory meets network security and privacy[R]. [S. l.]: ACM Computing Surveys,2011.

[12] AFRAND A, DAS S K, BASU K, *et al*. Intrusion detection in sensor networks: a non-cooperative game approach network computing and applications[C]//Proc of the 3rd IEEE International Symposium on Network Computing and Application. Washington DC: IEEE Computer Society,2004:343-346.

[13] KANTZAVELOUA I, KATSIKAS S. A game-based intrusion detection mechanism to confront internal attackers[J]. Computers & Security,2010,29(8):859-874.

[14] 周四清,李志艳,刘田. 无线传感器网络入侵检测的重复博弈建模研究[J]. 计算机工程与应用,2009,45(3):119-123.

[15] McKELVEY R D, McLENNAN A M, TUROCY T L. Gambit: software tools for game theory[EB/OL]. (2007-01-30). [2009-01-20]. http://gambit.sourceforge.net.

(上接第 1529 页)

图 5 中的颜色集,定义如下

$C(p_1)=\{d_{11}\}, C(p_2)=\{d_{21}\}, C(p_3)=\{d_{31},d_{32}\}, C(p_4)=\{d_{41}\}, C(p_5)=\{d_{51}\}, C(p_6)=\{d_{61},d_{62}\}, C(p_7)=\{d_{71}\}, C(p_8)=\{d_{81}\}, C(p_a)=\{d_{a2}\}, C(p_b)=\{d_{b2}\}, C(p_c)=\{d_{c2}\}, \mu_j=\{\mu_1,\mu_2,\mu_3,\mu_4\}$。

将上述数据用于本文的推理算法进行攻击实例推理,可得 d_{a2} 命题的 $w_{a2}=0.7$,说明攻击者提升了攻击权限,并且该节点以 0.7 的高可信度对后续攻击起促进作用;d_{b2} 命题的 $w_{b2}=0.63$,说明主机被植入僵尸程序,可信度为 0.63;命题 d_{c2} 的 $w_{c2}=0.567$,说明目标主机处于 DDoS 的攻击状态,可信度为 0.567。

4　结束语

本文提出了一种基于双枝模糊逻辑和着色 Petri 网的网络攻击模型,该模型的知识表示具有网络模型简明、容易实现的特点,对于处理网络攻击中的不确定知识具有一定的优势。从攻击和防御两方面对网络攻击进行综合考虑分析,并给出了 BBFCPN 模型的推理规则和推理算法。基于 BBFCPN 模型的推理算法不仅推理过程简单直观,而且还具有并行推理能力。实验结果表明,该模型能清晰表示网络攻击和防御情况,推理算法是有效可行的。

参考文献:

[1] 任丹丹,杜索果. 一种基于攻击树的 VANET 位置隐私安全风险评估的新方法[J]. 计算机应用研究,2011,28(2):728-732.

[2] 吴金宇,金舒原,杨智. 基于网络流的攻击图分析方法[J]. 计算机研究与发展,2011,48(8):1497-1505.

[3] 冯萍慧,连一峰,戴英侠,等. 面向网络系统的脆弱性利用成本估算模型[J]. 计算机学报,2006,29(8):1375-1381.

[4] 陈锋,刘德辉,张怡,等. 基于威胁传播模型的层次化网络安全评估方法[J]. 计算机研究与发展,2011,48(6):945-954.

[5] 黄光球,赵阿妮,任大勇. 用双枝模糊逻辑和模糊 Petri 网构建的攻击模型[J]. 计算机工程与应用,2010,46(2):99-103.

[6] 刘刚,徐衍亮,赵建辉,等. 双枝模糊逻辑[J]. 计算机工程与应用,2003,39(30):96-98.

[7] 刘刚,赵建辉,刘强. 双枝模糊逻辑(Ⅱ)[J]. 计算机工程与应用,2005,41(19):47-49,107.

[8] 史开泉,李岐强. 双枝模糊决策与决策识别问题[J]. 中国工程科学,2001,3(1):71-77.