基于博弈论的移动 Ad hoc 网络入侵检测模型

李奕男 钱志鸿 刘 影 张 旭
(吉林大学通信工程学院 长春 130025)

摘 要：随着计算机技术尤其是网络技术的发展，人们面临着由于入侵而带来的一系列安全问题。该文将博弈理论引入到移动 Ad hoc 网络入侵检测系统中，建立网络安全博弈模型，经过理论推导和仿真实验得到该模型的纳什均衡解。实验结果表明，该模型有效地提高了检测率，降低了误检测率，网络开销较小，证明该方法的有效性和可行性。

关键词：Ad hoc 网络；博弈论；入侵检测系统
中图分类号：TP393.08 **文献标识码**： A **文章编号**：1009-5896(2010)09-2245-04
DOI: 10.3724/SP.J.1146.2010.00225

An Intrusion Detection Model of Mobile Ad hoc Networks Based on Game Theory

Li Yi-nan Qian Zhi-hong Liu Ying Zhang Xun
(*School of Jilin University of Communication Engineering*, *Changchun* 130025, *China*)

Abstract: With development of computer technology, especially Internet technology, people are faced with the invasion brought about a series of security problems. Employing game theory into a mobile Ad hoc network Intrusion Detection System (IDS) is presented in this paper. Network security game model is established, theoretical analysis and experiments of the Nash equilibrium solution of the model is yielded in this paper. Experimental results show that the model has effectively improved the detection rate and reduce the false detection rate, bringing the smaller network overhead. The effectiveness and feasibility of the method are proved.

Key words: Ad hoc network; Game theory; IDS (Intrusion Detection System)

1 引言

随着计算机网络技术的不断深入发展，移动计算设备和移动通信设备的广泛应用，给人们在信息资源的利用和共享带来了巨大的便利。移动 Ad hoc 网络(MANET)是由一组带有无线收发装置的移动终端组成的多跳、临时性自治系统，通过传输范围有限的移动节点间的互相协作和自我组织保持网络的互联和数据传输。Ad hoc 网络具有无中心控制的分布性、动态变化的拓扑结构和多跳的路由结构等特性，已经广泛的应用于军事通信、灾难救助和临时应急会议通信等应用环境[1]。

Ad hoc 网络技术拥有广阔的应用前景，但是由于它的无线通信信道的完全开放性和网络拓扑结构频繁变化缺乏稳定性，使得 Ad hoc 网络更容易受到从被动监听到主动扮演、消息重放、篡改报文和拒绝服务等各种安全威胁和攻击[2]，因此移动 Ad hoc 网络入侵检测系统(IDS)就成为网络安全方案的第二道防火墙。

移动 Ad hoc 网络与现有的固定网络相比有很大的差异，因此那些在传统计算机网络中已经广泛应用的安全机制不再适用于移动 Ad hoc 网络。入侵检测系统的主要作用就是对整体网络进行全面监控，实时检测是否发生了入侵事件，并根据已有的安全策略对入侵事件进行判断和响应。但是现有的入侵检测手段还很有限，当攻击者改变攻击策略时，入侵检测系统反应明显滞后。同时，入侵检测系统本身报警数量大、误报率高的问题也很突出，使得检测结果并不完全可信。本文将博弈理论引入到移动 Ad hoc 网络的入侵检测系统中，针对多攻击节点和不同强度的攻击源，建立一个非协作博弈入侵检测模型。通过引入博弈论模型，建立攻防双方博弈模型，本文论证了该博弈存在一个纳什均衡，能够实现网络整体安全性的定量分析。仿真实验表明该模型通过较小的代价换取整体网络的安全运行，具有良好的性能指标，证明了该方法的正确性和可行性。

针对攻防双方不对称的网络安全问题，

2010-03-11 收到，2010-05-25 改回
教育部高等学校博士学科点专项科研基金(20090061110043)和国家自然科学基金(60940010)资助课题
通信作者：李奕男 dce_master@163.com

Musman 和 Ding Yong[3,4]等人提出了静态映射型入侵响应模型。该模型是指按一定的原则对攻击进行分类，并用人工的方式将每一次报警映射到一个预先定义好的相应措施上。静态映射型入侵响应很大程度上解决了人工响应长、负担大的问题，但是当系统状态发生变化，如网络拓扑结构和网络负载发生变化时，原有的响应措施将不再适应。在此基础上，Carver 和 Ragsdale[5,6]等人在 2000 年提出了通过考虑 IDS 自身的误报警率和以往响应方式的成功率来自动调整响应映射。这种动态自适应方法部分解决了响应措施的适应性问题，但是因为没有考虑响应的代价，使得有时响应会得不偿失。2002 年 Lee 和 Fan[7]等人提出了基于系统收益的入侵检测响应模型，在综合计算操作代价、响应代价和损失代价的基础上选择适当的应对策略。这种收益模型未能将不同系统遭受同一攻击的损失不同区别开来，收益考虑的不全面。Foo 和 Wu[8]提出了根据 IGraph 图法的基于系统收益的入侵响应和容忍模型，对系统可能的入侵路径进行描述，然后根据入侵可能造成的系统损失和响应代价选择响应措施。这种方法非常复杂不易实现，实用性不高。Lye 和 Wing[9]使用统一和随机博弈对系统中的攻防双方关系进行了描述和推理，证明了博弈理论对入侵检测和响应的适用性。Xu[10]等人通过博弈理论框架来对他们提出的 DDOS 防御系统的性能进行分析，引导防御系统的调整。

2 移动 Ad hoc 网络入侵检测博弈模型

2.1 博弈论与网络入侵和响应

对于分布式网络的入侵响应而言，响应者所期望的结果或者所采取的行动，不只取决于其自身的行为(策略)，还应取决于入侵者和检测系统的行为(策略)，而博弈论正是研究这种策略互相依存的理论。博弈论是研究竞争条件决策分析的科学，它研究的典型问题是若干个利益冲突者在同一环境中进行决策以求自己的利益得到满足[11]。在网络入侵和响应的过程中，入侵者的目的就是对网络发起进攻，非法获得网络信息，影响正常的网络服务；防御响应一方就是要通过实施安全策略保证网络的正常服务。因此，入侵者和响应者之间的博弈是利益冲突的博弈，双方都希望能够最大化自己的利益，攻防双方之间强调个人的理性。因此，入侵者和响应者之间的利益是完全对立的，网络入侵和响应的过程是一个非合作、完全信息、有限次重复的对抗性博弈。

2.2 博弈模型

博弈问题有 5 个要素：局中人，策略空间，概率分布，信息集，效用函数。

定义 假设 Ad hoc 网络中有 N 个节点($n=1,\cdots,N$)，则基于博弈的 Ad hoc 网络入侵检测模型如下：

$$\Gamma=\{\{A,D\},\{S_A,S_D\},\{P_A,P_D\},\{I_A,I_D\},\{R_A,R_D\}\} \quad (1)$$

局中人：式(1)中 $\{A,D\}$ 表示局中人，A 表示网络攻击方，即网络入侵者；D 表示网络防御方，即 IDS 的响应的决策者。

策略空间：式(1)中 $\{S_A,S_D\}$ 表示局中人的策略空间，S_A 表示攻击方的策略，S_D 表示防御方的策略 。

概率分布：式(1)中 $\{P_A,P_D\}$ 表示探测器的概率分布矩阵，其中 $\sum_{j=1}^{N}\sum_{i=1}^{N}(P_{A_i},\ P_{D_j})=1$ 。

信息集：式(1)中 $\{I_A,I_D\}$ 表示攻击方和防御方的信息集，信息集的维数由攻击方采用的攻击方式数决定。

效用函数：式(1)中 $\{R_A,R_D\}$ 表示博弈模型的效用函数，代表阶段博弈结束后，攻防双方可能得到的收益集合。

2.3 模型存在纳什均衡的证明

根据纳什定理[12]：在一个有 n 个博弈方的博弈 $G=\{S_1,S_2,\cdots,S_n;u_1,u_2,\cdots,u_n\}$ 中，如果 n 是有限的，且 S_i 是有限集($i=1,2,\cdots,n$)，则该博弈至少存在一个纳什均衡。即每一个有限策略博弈都至少有一个混合策略纳什均衡。

本模型攻防双方的信息集维数是有限的，因此对应的策略型博弈也是有限的。根据纳什均衡的存在条件，任意有限策略型博弈至少存在一个策略纳什均衡。博弈中局中人都是理性的，攻防双方只有在达到纳什均衡的策略下，才能使收益最大化，也即局中人的最佳选择。

3 仿真结果与分析

为了验证本论文提出模型的准确性，选用了 NS-2[13]软件对模型进行仿真。实验中引入了两种实验场景：(1)正常的具有入侵检测系统的 AODV 路由协议；(2)引入了基于博弈论的入侵检测的改进 AODV 路由协议。通过测量系统的检测率、误检测率、路由包开销和平均延迟 4 个主要参数指标来真实反映模型系统的安全性和稳定性。具体实验参数设置如表 1 所示。实验结果如图 1 所示。

从图 1(a)和图 1(b)的仿真结果可以看出，随着网络中恶意节点数目的增加，大规模入侵事件的发生，IDS 会产生大量警报，造成警报泛洪，从而会占用大量的通信带宽，影响正常的网络通信，网络的整体性能呈现下降趋势。本文提出的入侵检测模

表 1 NS-2 参数设置

节点个数(个)	200
仿真区域(m^2)	1000×1000
仿真时间(s)	1200
路由协议	AODV
MAC 类型	IEEE802.11
节点移动模式	随机运动
传输距离(m)	250
最大移动速度(m/s)	20
数据包大小 (B)	256
数据包转发率(pps)	4
攻击方式	Ad hoc flooding

型既可以提高准确率，又能够缓解网络拥塞的状况。实验证明其具有很高的检测率，达到 90%以上，误检率保持在 10%以下，证明了方法的有效性。

从图 1(c)的仿真结果可以看出，本模型计算量少，给系统带来的路由开销小，占用带宽少，节省了网络资源。从图 1(d)中可以发现本模型计算时间短，检测效率高，非常适宜移动 Ad hoc 网络。

4　结论

本文提出了一种基于博弈论 Ad hoc 网络入侵检测模型，将攻防双方的网络入侵和响应的过程抽象成一个非合作、完全信息、有限次重复的对抗性博弈。在双方的博弈过程中，寻求纳什均衡，使局中人进行最佳选择。通过实例分析和实验可以看出，该模型能够使 IDS 在响应后的收益得到保证，并且最优解稳定可靠。

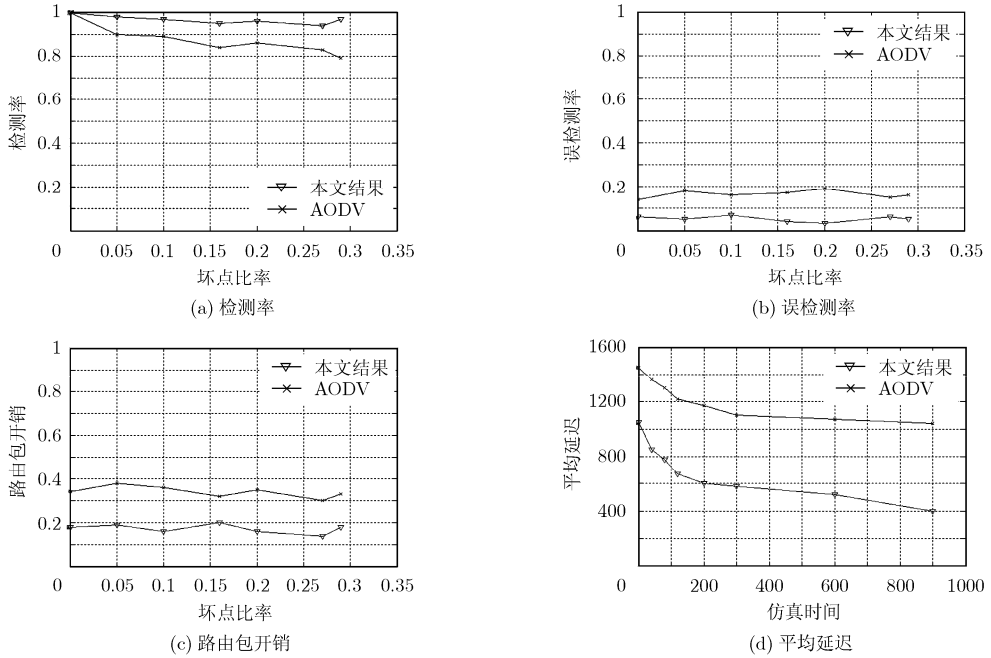

图 1 采用博弈论的入侵检测的仿真结果

参 考 文 献

[1] 朱建明, Srinivasan Raghunathan. 基于博弈论的信息安全技术评价模型[J]. 计算机学报, 2009, 32(4): 828–834.
Zhu Jian-ming and Srinivasan Raghunathan. Evaluation model of information security technologies based on game theoretic[J]. *Chinese Journal of Computers*, 2009, 32(4): 828–834.

[2] Ryu Y U and Rhee H S. Evaluation of intrusion detection systems under a resource constraint. *ACM Transactions on Information and Systems Security*, 2008, 11(4): 20.1–20.24.

[3] Musman S and Flesher P. System or security managers' adaptive response tool [C]. DARPA Information Survivability Conference and Exposition 2000, Hilton Head, USA, 2000, Vol.2: 1056–1060.

[4] 丁勇, 虞平, 龚俭. 自动入侵响应系统的研究[J]. 计算机科学，2003, 30(10): 160–166.
Ding Yong, Yu Ping, and Gong Jian. A study of automated intrusion response systems [J]. *Computer Science*, 2003, 30(10): 160–166.

[5] Carver C, Hill J M, and Surdu J R. A methodology for using intelligent agents to provide automated intrusion response[C]. The IEEE Systems, Man, and Cybernetics Information

Assurance and Security Workshop, West Point, NY, 2000: 110–116.

[6] Ragsdale D, Carver C, and Humphries J, *et al*.. Adaptation techniques for intrusion detection and intrusion response system[C]. The IEEE Int'l Conf on Systems, Man, and Cybernetics at Nashville, Tennessee, 2000: 1398–1406.

[7] Lee W, Fan W, and Miller M, *et al*.. Toward cost-sensitive modeling for intrusion detection and response [J]. *Journal of Computer Security*, 2002, 10(1/2): 5–22.

[8] Foo B, Wu Y, and Mao Y, *et al*.. ADEPTS: adaptive intrusion response using attack graphs in an E-commerce environment[C]. Int'l Conf on Dependable Systems and Networks (DSN'05), Washington, 2005: 139–146.

[9] Lye K and Wing J M. Game strategies in network security[C]. The 2002 IEEE Computer Security Foundations Workshop, Copenhagan, Denmark, 2002: 71–86.

[10] Xu J and Lee W. Sustaining availability of Web services under distributed denial of service attacks [J]. *IEEE Transactions on Computer*, 2003, 52(4): 195–208.

[11] [美]艾里克 •拉斯缪森. 王晖等译. 博弈与信息博弈论概论. 北京: 北京大学出版社, 2003: 385–417.

[12] 董武世, 孙强, 柯宗武, 陈年生. 基于博弈论的 Ad hoc 网络功率控制模型[J]. 武汉理工大学学报, 2009, 31(17): 114–122.
Dong Wu-shi, Sun Qiang, Ke Zong-wu, and Chen Nian-sheng. Power control model based on game theory in Ad hoc networks[J]. *Journal of Wuhan University of Technology*, 2009, 31(17): 114–122.

[13] Ns2 network simulation[OL]http ://www.isi.edu/nsnam/ns , 2009.

李奕男： 男，1978 年生，博士生，研究方向为无线短距离通信、Ad hoc 网络安全.

钱志鸿： 男，1957 年生，教授，博士生导师，从事领域为无线网络通信系统的信号分析和处理、通信系统微弱信号检测理论与应用.

刘 影： 女，1983 年生，博士生，研究方向为无线传感器网络定位.

张 旭： 男，1982 年生，博士生，研究方向为无线自组织网络的 QoS 机制研究.