基于博弈的无线传感器网络入侵检测模型

熊自立 韩兰胜 徐行波 付 才 刘布雨
(华中科技大学计算机科学与技术学院 武汉 430074)

摘 要 无线传感器网络的广泛应用扩展了人们获取信息的能力,但是其固有的网络特点使得其更容易遭受网络攻击。现有的入侵检测系统通常只针对特定的攻击方式,对其他的攻击则无能为力。另外增加的能量消耗降低了网络的使用寿命。由此,以博弈论为理论基础,对无线传感器网络中的攻防过程进行分析,通过分析模型均衡解来论证执行入侵检测系统的必要性。针对网络入侵者攻击手段的多样性问题,对博弈模型进行深化改进,建立非合作完全信息静态博弈模型,通过分析模型的混合纳什均衡解,得出入侵检测系统的最佳防守策略,平衡了系统的能量消耗和检测效率。仿真实验结果表明,基于博弈的无线传感器网络入侵检测系统不仅能够有效地抵御多种网络攻击,而且降低了入侵检测系统所引起的能量消耗,延长了网络的使用寿命。

关键词 无线传感器网络,入侵检测,博弈理论
中图法分类号 TP311 **文献标识码** A

Research on Intrusion Detection of Wireless Sensor Networks Based on Game Theory

XIONG Zi-li HAN Lan-sheng XU Xing-bo FU Cai LIU Bu-yu
(School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract Wide application of wireless sensor networks extends people's ability to obtain information, but its inherent network characteristics make it more vulnerable to cyber-attack. Current intrusion detection systems are against for specific attacks, but powerless for other attacks and consump a little high energy, thus reduce the lifetime of the network. The paper proposed an intrusion detection model based on game theory, in which the attack-defense process between intrusion detection system and attacker is looked as a non-cooperative game model. To deal with the problem of diversity network intruder attacks, game model has been improved and established a non-cooperative information static game model. By analyzing the model's mixed Nash equilibrium, the optimal defense strategy is obtained. It can balance the detection efficiency and energy consumption of the system. The simulation results show that the intrusion detection system based on game theory not only can resist a variety of network attacks effectively, but also reduce the energy consumption and prolong the lifetime of the network.

Keywords Wireless sensor networks, Intrusion detection, Game theory

1 无线传感器网络安全及博弈论概述

1.1 无线传感网络概述

随着嵌入式技术、传感技术及无线通信技术的飞速发展,人类迫切需要丰富多样的计算机通信设备来获取准确可靠的信息。无线传感器网络(Wireless Sensor Network, WSN)是由大量智能、微型、廉价的传感器节点通过无线通信方式自组织形成的一个多跳网络[1-2],主要由 3 个部分组成:传感节点、基站(Base Station, BS)和观察者[3]。传感节点通常以空投的形式随机部署在待监测区域中,通过传感部件采集信息后将其发送给基站。基站负责对所有节点的汇聚信息进行分析和筛选,将有用的信息通过网络传递给观察者[3]。观察者通过网络获取到所需要的数据后,就可以对数据进行分析,达到自己的监测目的。

目前国内外针对无线传感器网络的安全研究可以分为 3 类:密钥管理、认证和安全路由、安全服务[4]。现有的安全研究不能消除大部分的安全攻击[3]。入侵检测系统(Intrusion Detection System, IDS)作为安全防范的第二道设施,是安全防护机制的合理补充,它采用的是一种主动的检测技术,能够有效地发现入侵行为,并进行积极的响应,是无线传感器网络中应对广泛安全攻击的一个解决方案。

入侵是指在非授权的情况下,试图破坏网络系统的正常运行或损害传感器节点的非法活动。入侵检测系统就是在不同的网络层次监测用户的行为或网络的流量[4]。目前无线传感器网络中的入侵检测算法可以分为两大类:误用检测(Signature-based,即基于误用的 Misuse-based)和异常检测(Anomaly-based,即基于行为的 Behavior-based)[5]。误用检测算法根据检测规则只对特定的攻击手段具有较高的检测

本文受国家自然科学基金项目:基于任务的木马关联任务识别研究(61272033),国家自然科学基金项目:移动网络行为的多态聚类及其演化研究(61270335),国家自然科学基金项目:恶意代码的多态图谱及隐式空间研究(61572222)资助。
熊自立(1960—),男,硕士生,工程师,主要研究方向为计算机网络,E-mail:xzili@hust.edu.cn;韩兰胜(1972—),男,博士,副教授,主要研究方向为网络空间安全、大数据安全,E-mail:hanlansheng@hust.edu.cn(通信作者);徐行波(1991—),男,硕士生,主要研究方向为网络信息安全、无线传感器网络。

率，对其他的攻击方式则无能为力；异常检测算法虽然能够检测多种攻击方式，但需要大量的历史数据进行学习训练，很难提高效率。混合式的入侵检测机制将上述两者综合[6]，但是两者的衔接是该检测机制的一个难题。WSN 中现有的入侵检测系统大多部署在所有的传感器节点中，或是将网络划分为簇状结构，然后在簇头节点中部署运行 IDS，并没有过多地考虑能耗问题[7]。虽然有一些入侵检测系统将博弈论应用到 IDS 的决策过程中，用以降低能量的消耗[8]，但是这些博弈模型大多只考虑单次博弈过程，并假设攻击者只有一种攻击手段[9]。而在实际的无线传感器网络环境中，攻防博弈过程大部分是多次的，攻击的手段可能是多种多样的，该模型显然不能满足实际的需要[10-11]。

1.2　博弈论概述

博弈论是研究对抗现象的一种数学理论，其考虑的是博弈过程中个体的预测行为和实际行为[12]。参与博弈的个体均具有不同的目标或利益，为了使各自利益达到最大化，各方必须考虑对手的各种可能的行动方案，并选择对自己最有利或最合理的方案，为方便后续描述，结合本文问题对博弈论的几个基本概念进行定义。

定义 1（参与者）　指一个博弈中的决策主体，通过合理地选择自己的行动，以期取得最大化的收益（或效用）。通常用 $i=1,2,\cdots,n$ 来表示。

定义 2（信息）　指参与者在博弈过程中能了解和观察到的知识，这些知识包括参与者的个数、特征和行动等。

定义 3（策略空间）　策略是参与者如何对其他参与者的行为做出反应的行动规则，它规定参与者在什么时候选择什么行为。通常 S_i 表示参与者 i 的一个特定策略，n 维向量 $S=\{S_1,S_2,\cdots,S_n\}$ 即称为一个策略组合。

定义 4（收益）　在博弈论中，收益是参与者在一个特定的策略组合下得到的确定的效用或者期望效用。效用通常表现为博弈结果的输赢、得失、盈亏。效用必须能用数值表达其大小，通常用 U_i 表示参与者 i 的收益，如果一个战略组合是 $(S_1,S_2,\cdots,S_n)$，那么每个参与者的收益可表示为 $U_i=U_i(S_1,S_2,\cdots,S_n)$，$i=1,2,\cdots,n$。

定义 5（均衡）　在博弈论中，均衡是所有参与者的最优策略组合。通常记为 $S^*=(S_1^*,\cdots,S_2^*,\cdots,S_n^*)$，$S_i^*$ 是参与者 i 在均衡状态下的最优策略，它是参与者 i 所有可能的策略中使 U_i 最大化的策略。

对于不同类型、不同条件的博弈问题可以形成各种各样的、特定的均衡概念。纳什均衡是指在一策略组合中，任一参与者的决策都是相对其他参与者决策的最优值，在此种情况下，没有参与者愿意单独偏离决策为他选定的策略。

根据相互发生作用的当事人之间是否有约束力的协议，可以分为合作博弈和非合作博弈。由于合作博弈比非合作博弈更复杂，在理论上的成熟度远不如非合作博弈，因此博弈论中用的最多的就是非合作博弈。

2　基于博弈的入侵检测模型研究

2.1　基于博弈的入侵检测模型

攻击者为了获取利益而试图攻击传感器网络节点，入侵检测系统为了维护系统的正常运转而检测入侵程序，显然这是一个相互对立的博弈过程。攻击者每次发起攻击都需要付出一定的代价，攻击成功便会获取一定的收益；入侵检测系统每次开启都会消耗节点的能量，检测成功也会获得相应的收益。为此通过博弈模型来模拟网络的攻防过程，找出攻击者和入侵检测系统之间的均衡解，解决入侵检测系统面临的能耗问题和性能问题。

2.1.1　博弈模型的建立

显然攻击者和入侵检测系统之间不存在合作的可能，应该选择非合作博弈模型。在攻防过程中，攻击者和检测者之间不断重复攻防过程，显然这是一个重复博弈。在每一次博弈中，攻击者和检测者之间的行动并没有固定的先后顺序，二者有可能同时行动，也可随机先后行动，但是后行动者对先行动者采取的策略一无所知，这又是一个静态博弈的过程。假设在博弈过程中，攻击者和检测者对彼此的特征、策略空间和收益函数等信息有准确的了解，博弈过程符合完全信息博弈。由此，我们可以选定博弈模型为非合作完全信息静态博弈。

在无线传感器网络的攻防模型中，参与者主要是网络攻击者（Attacker，记为 A）和入侵检测系统（Defender，记为 D）。信息对于博弈双方来说都是完全可以感知的，也就是完全信息。不妨将其决策空间记为 SA 和 SD，其收益函数记为 UA 和 UD。模型的均衡解是由前面的 4 个因素分析推导出来的，这样博弈模型就可以简单地标记为：$G=\{(D,A),(SD,SA),(UD,UA)\}$。

由于无线传感器网络中的能量资源非常有限，不能在每个节点中运行 IDS，必须使用一种策略来平衡系统的能量消耗和检测性能。可以使用分簇路由协议将网络划分为簇。每个簇中都含有一个簇头节点（Cluster Head，CH）和若干个成员节点，成员节点主要负责收集信息并将其传递给簇头，簇头节点主要负责簇内信息的转发和执行入侵检测程序。簇头是通过簇内节点周期性的选举产生的，其本质上和簇中的成员节点一样，簇头中的 IDS 启动与否取决于基站的指令。

假设传感器网络中有 N 个节点，按照分簇路由协议划分为 k 个簇，分别记为 $C_1,C_2,\cdots,C_k$，每个簇中含有的节点数目为 $C_i(i=1,2,\cdots,k)$。我们假定攻击者在每次攻击中最多只能攻击一个簇，基站在每次防守时最多只能选择一个簇头启动 IDS，那么在每一次攻防博弈中，对于网络中的一个簇 C_i 来说，攻击者有 3 种策略：要么对簇 C_i 进行攻击（记为 A_1）；要么暂时不攻击，等待时间 t 后再进行攻击（记为 A_2）；要么在网络中选择另一个不同的簇 C_j 进行攻击（记为 A_3），也就是说 $SA=\{A_1,A_2,A_3\}$。对于防守者来说，其也有 3 种策略可供选择，要么对簇 C_i 进行保护（记为 D_1）；要么不启动 IDS（记为 D_2）；要么选择一个不同的簇 $C_j(i\neq j)$ 进行保护（记为 D_3），也就是说 $SD=\{D_1,D_2,D_3\}$。将 SA 和 SD 两两进行组合，便可以得到防御者和攻击者的所有策略组合，如矩阵 X 所示：

$$X=\begin{bmatrix}(D_1,A_1) & (D_1,A_2) & (D_1,A_3)\\ (D_2,A_1) & (D_2,A_2) & (D_2,A_3)\\ (D_3,A_1) & (D_3,A_2) & (D_3,A_3)\end{bmatrix} \tag{1}$$

其中，矩阵的行代表防守者，列代表攻击者。为了确定攻击者和防御者的收益函数，需要定义一些符号，如表 1 所列。

表 1　符号的定义

符号	含义
$U(t)$	t 时刻传感器网络正常运转的收益
Avg	网络中每个节点的平均价值
$C_i(t)$	t 时刻入侵检测系统保护簇 C_i 的代价
$V_i(t)$	t 时刻入侵检测系统保护簇 C_i 成功的收益
$Q_i(t)$	t 时刻攻击者攻击簇 C_i 付出的代价
$P_i(t)$	t 时刻攻击者攻击簇 C_i 成功获取的收益
$W(t)$	攻击者暂时不攻击，等待下一次攻击的代价

$X_{11}=(D_1,A_1)$表明攻击者选择网络中的簇 C_i 进行攻击，IDS 同样选择簇 C_i 进行保护。假定当攻击者和防守者选定同一个簇时，IDS 一定可以检测出入侵。那么此时攻击者必定攻击失败，其为了攻击簇 C_i 付出的代价为 $Q_i(t)$，得到的收益为 0，此时 $UA=-Q_i(t)$；防守者必定防守成功，其为了防守簇 C_i 付出的代价为 $C_i(t)$，得到的收益为 $V_i(t)$，外加系统正常运转 $U(t)$，这里需要说明的是 $V_i(t)$ 为防御成功的收益，它是相对于 C_i 被破坏造成的损失而言的。而系统正常运转的收益 $U(t)$ 是整个传感器网络运转的收益，并不包括在 $V_i(t)$ 中，故 $UD=U(t)+V_i(t)-C_i(t)$。

同理可分析其他，最后整理出攻击者的收益矩阵 Y 和防守者的收益矩阵 Z，如式(2)所示：

$$Y=\begin{bmatrix} -Q_i(t) & -W(t) & P_j(t)-Q_j(t) \\ P_i(t)-Q_i(t) & -W(t) & P_j(t)-Q_j(t) \\ P_i(t)-Q_i(t) & -W(t) & -Q_j(t) \end{bmatrix} \tag{2}$$

$$Z=\begin{bmatrix} U(t)+V_i(t)-C_i(t) & U(t)-C_i(t) & U(t)-C(t)-C_j(t)*Avg \\ U(t)-C_i'(t)*Avg & U(t) & U(t)-C_j'*Avg \\ U(t)-C_j(t)-C_i'(t)*Avg & U(t)-C_j(t) & U(t)+V_j(t)-C_j(t) \end{bmatrix} \tag{3}$$

其与防御者和攻击者的策略组合矩阵式(1)相对应，在矩阵 Y 和 Z 中，行号和列号分别代表防御者和攻击者所选择的策略。

2.1.2 纳什均衡解分析

有了收益函数矩阵，在参与者双变量收益矩阵给出的情况下，寻求纳什均衡解的一个最简单的办法为划线法。划线法的核心思想是：对于参与者 2 的每一个特定策略，也就是在双变量矩阵的每一列中，找出参与者 1 的最优策略(收益最大值)，并在相应的收益下划横线；然后在双变量矩阵的每一行中，找出参与者 2 的最优策略(收益最大值)，并在其下划横线；最后，如果双变量矩阵中某一个单元的两个收益值下都被划了横线，那么这个单元对应的策略组合就是该博弈的一个纯战略纳什均衡。

矩阵 Y 和 Z 本可以合并成一个双变量矩阵，但是由于页面宽度有限，合并后的矩阵放不下，因此就拆分成了两个矩阵，但是这并不妨碍我们使用划线法来求解博弈的纳什均衡解。对于攻击者的收益矩阵 Y 而言，即在每一行中找出收益的最大值；对于防守者的收益矩阵 Z 而言，即在每一列中找出收益的最大值。

攻击者攻击簇 C_i 成功获取的收益为 $P_i(t)$，付出的代价为 $Q_i(t)$，很显然收益大于代价，也即 $P_i(t)>Q_i(t)$，否则若攻击者作为一个理性的博弈人，是不会选择攻击的。攻击者攻击簇 C_i 成功获取的净收益和攻击簇 C_j 成功获取的净收益本质上没有太大的区别，也即：$P_i(t)-Q_i(t)\approx P_j(t)-Q_j(t)$。因此，在矩阵 Y 中，第一行的收益最大值为 y_{13}，第二行的收益最大值为 y_{21} 或 y_{23}，第三行的收益最大值为 y_{31}。

矩阵 Z 很显然是一个对称矩阵，入侵检测系统成功地在簇 C_i 上检测到入侵的收益为 $V_i(t)$，启动检测系统付出的代价为 $C_i(t)$，很显然 $V_i(t)>C_i(t)$。因此，在矩阵 Z 中，第一列的收益最大值为 Z_{11}。由于矩阵是对称的，因此第三列的收益最大值为 Z_{33}。很显然，矩阵第二列的收益最大值为 Z_{22}。

矩阵 Y 中行收益最大值分别为 y_{13}，y_{21} 或 y_{23}，y_{31}，矩阵 Z 中列收益最大值分别为 z_{11}，z_{22} 和 z_{33}。由于两个矩阵中收益最大值的下标并不是完全相同的，因此可以得到如下结论。

结论 1 该博弈模型没有纯策略纳什均衡。

这也正符合我们的预期，因为如果该博弈存在纳什均衡解，那么攻防双方就会选定均衡解不动摇。假设攻击者的最优解是攻击簇 C_i，防守者的最优解是防守簇 C_j，由于攻击者攻击簇 C_i，那么对于防守者来说，防守簇 C_i 显然会比防守簇 C_j 获取更多的收益，显然防守簇 C_j 并不是防守者的最优解，这会促使防守者防守簇 C_i。当防守者防守簇 C_i 时，会使得攻击者攻击簇 C_i 失效，攻击者的收益会减少，攻击者为了获取更多的利益，显然会重新选择一种攻击策略。攻防双方无法稳定下来，因此该博弈没有纯战略纳什均衡。

结论 2 博弈过程中攻击者为了获取最大收益总是选择攻击。虽然没有均衡解，但是我们知道，矩阵 Y 中行收益最大值分别为 y_{13}，y_{21} 或 y_{23}，y_{31}。通过分析列下标可以发现列下标为 1 和 3，也就是说，不管防守者选择什么策略，对于攻击者来说，其为了获取最大收益值，总是会选择策略 A_1 和 A_3，即攻击者总会发起攻击。在攻击者选择为了利益发起攻击的前提下，再来分析防守者矩阵 Z 的第一列和第三列。通过观察发现，防守者为了获取最大收益，总是试图找出攻击者要攻击的簇，然后进行保护。

2.2 多攻击检测博弈模型

对于大多数常见攻击，目前已经有了相匹配的入侵检测规则，直接使用误用检测即可以较高的准确率检测入侵；对于新型攻击，由于攻击者的攻击特性尚不可知，此时入侵规则匹配法已经不再适用，我们需要使用异常检测来判断入侵。误用检测所需要采集的数据特征和异常检测所需要采集的数据特征不尽相同，不能简单地将这两个检测模块串联起来。对于只遭受一种攻击的网络来说，多收集数据意味着更多的能量消耗，逐次通过各个模块意味着更多的检测时间。因此，将这两个检测模块并列起来，在每次检测过程中只使用一种检测模块。但是这就需要我们研究出一种策略，用以指导入侵检测部分在正确的时间使用正确的检测模块。

接下来将通过建立攻击者和防守者的博弈模型，分析寻求指导入侵检测部分模块开启的最优策略。

2.2.1 博弈模型的建立

不妨将本次博弈模型记为 G_1。博弈的参与者依然为攻击者和防守者，分别记为 A 和 D。对于攻击者来说，其攻击策略有两种：1)选择常用攻击手段(记为 A_1)；2)选择新型攻击手段(记为 A_2)。对于防守者来说，其也有两种防守策略：1)使用误用检测开启 IDS(记为 D_1)；2)使用异常检测启动 IDS(记为 D_2)。为了后文计算方便，我们用 $U_{ij}(D)$ 表示防守者选择策略 D_i、攻击者选择策略 A_j 时防守者的收益，用 $U_{ij}(A)$ 表示此时攻击者的收益，用 U_A 表示攻击者的总收益函数，用 U_D 表示防守者的总收益函数。则攻防博弈函数可以表示为：

$$G_1=\{(D,A),(S_D,S_A),(U_D,U_A)\} \tag{4}$$

其中，$S_D=\{D_1,D_2\}$，$S_A=\{A_1,A_2\}$。博弈的策略矩阵为 M，如式(5)所示：

$$M=\begin{bmatrix} (D_1,A_1) & (D_1,A_2) \\ (D_2,A_1) & (D_2,A_2) \end{bmatrix} \tag{5}$$

假设使用误用检测方法检测常见攻击的平均检测准确率

为 α，使用异常检测方法检测新型攻击的平均检测准确率为 β，根据 1.1 节中对误用检测和异常检测的定义，使用异常检测方法检测常见攻击和使用误用检测方法检测新型攻击的准确率均为 0。因此可以算出各个节点攻击者和入侵者的收益函数。

当 $M_{11}=(D_1,A_1)$ 时，攻击者选择使用常见的攻击手段进行攻击，防守者使用误用检测方法进行入侵检测，由于此时的检测准确率为 α，因此

$$U_{11}(A)=(1-\alpha)(P_i(t)-Q_i(t))-\alpha Q_i(t)$$
$$=(1-\alpha)P_i(t)-Q_i(t)$$
$$U_{11}(D)=\alpha(U(t)-C_i(t))+(1-\alpha)(U(t)-C_i(t)-C_i'*Avg)$$
$$=U(t)-C_i(t)-(1-\alpha)C_i'*Avg$$

攻击者攻击簇 i 获取的收益 $P_i(t)$ 等于簇 i 沦陷时的损失 $C_i'*Avg$，所以上述防守者的收益可以化解为：$U_{11}(D)=U(t)-C_i(t)-(1-\alpha)P_i(t)$。

同理可分析得到其他 3 组数据，整理便可得到博弈的双变量收益矩阵：

$$Y'=\begin{bmatrix}(1-\alpha)P_i(t)-Q_i(t) & P_i(t)-Q_i(t)\\ P_i(t)-Q_i(t) & (1-\beta)P_i(t)-Q_i(t)\end{bmatrix}$$

$$Z'=\begin{bmatrix}U(t)-C_i(t)-(1-\alpha)P_i(t) & U(t)-C_i(t)-P_i(t)\\ U(t)-C_i(t)-P_i(t) & U(t)-C_i(t)-(1-\beta)P_i(t)\end{bmatrix}$$

其中，矩阵 Y' 表示攻击者的收益矩阵，矩阵 Z' 表示防守者的收益矩阵。在这两个矩阵中，行用来表示攻击者的策略，列用来表示防守者的策略。

为了得到防守者的防守策略，假设防守者以概率 p 执行误用检测，以概率 $1-p$ 执行异常检测；攻击者以概率 q 使用常用的攻击方式进行攻击，以概率 $1-q$ 使用新的攻击方式进行攻击。我们所求为当 (p,q) 为何值时，攻击者和防守者得到的收益最大。为此，可以根据上面的双变量收益矩阵，分别得出防守者和攻击者的总收益函数 U_D 和 U_A。

$$U_D=pqU_{11}(D)+p(1-q)U_{12}(D)+(1-p)qU_{21}(D)+(1-p)(1-q)U_{22}(D)$$
$$U_A=pqU_{11}(A)+p(1-q)U_{12}(A)+(1-p)qU_{21}(A)+(1-p)(1-q)U_{22}(A)$$

将上述矩阵 Y' 和 Z' 中的 $U_{ij}(D)$ 和 $U_{ij}(A)$ 代入 U_D 和 U_A，得到：

$$U_D=U(t)-C_i(t)-p_i(t)[1-\alpha pq-(1-p)(1-q)\beta]$$
$$U_A=[1-pq\alpha-(1-p)(1-q)\beta]P_i(t)-Q_i(t)$$

2.2.2　纳什均衡解分析

得到攻击者和防守者的总收益函数后即可分析其均衡解。由均衡解的定义可知，在均衡解处各方的收益函数达到最大值，可以使用极值法求出使 U_D 和 U_A 最大的策略。

在防守者的总收益函数 U_D 中，p 和 q 为变量，$\alpha,\beta,U(t),C_i(t),P_i(t)$ 均为常量，为了求得 p 值使 U_D 最大，可将 U_D 对 p 求偏导，并令其为 0，即：

$$\frac{\partial U_D}{\partial p}=[(\alpha+\beta)q-\beta]P_i(t)=0$$

得：$q=\frac{\beta}{\alpha+\beta}$。

同理，为了求得 q 值使 U_A 最大，将 U_A 对 q 求偏导并令其为 0，即：

$$\frac{\partial U_A}{\partial q}=[\beta-(\alpha+\beta)p]P_i(t)=0$$

得：$p=\frac{\beta}{\alpha+\beta}$。

那么，可以得到防守者的策略 S_D 为：

$$S_D=(p,1-p)=(\frac{\beta}{\alpha+\beta},\frac{\alpha}{\alpha+\beta})$$

即防守者以 $\frac{\alpha}{\alpha+\beta}$ 的概率采用误用检测算法进行入侵检测，以 $\frac{\alpha}{\alpha+\beta}$ 的概率采取异常检测方法进行入侵检测。

也可以得到攻击者的攻击策略 S_A 为：

$$S_A=(q,1-q)=(\frac{\beta}{\alpha+\beta},\frac{\alpha}{\alpha+\beta})$$

即攻击者以 $\frac{\beta}{\alpha+\beta}$ 的概率采用常见的攻击方法进行攻击，以 $\frac{\alpha}{\alpha+\beta}$ 的概率采用新型的攻击方法进行攻击。

上式中的 S_D 和 S_A 就是防守者和攻击者的纳什均衡解，在 p 和 q 取该值时，防守者和攻击者的收益达到最大值。可以对这个纳什均衡解做一个简单的分析：

当 α 一定时，β 越大，$p=q=\frac{\beta}{\alpha+\beta}$ 越大。β 越大，说明入侵检测系统中异常检测方法对新型攻击的检测率增加，这对攻击者来说意味着如果其使用新型攻击手段对网络进行攻击，将有很大的几率被检测出来，作为一个理性的博弈者，攻击者采用新型攻击手段进行攻击的概率将会降低，也即 $1-q=\frac{\alpha}{\alpha+\beta}$ 会减少，相应的攻击者采用常用攻击手段进行攻击的概率将会增大，也即 $q=\frac{\beta}{\alpha+\beta}$ 增大。当攻击者增大使用常用攻击进行攻击的频率时，对于防守者来说，其应该增大使用误用检测方法进行检测的概率，即 $p=\frac{\beta}{\alpha+\beta}$ 会增大，减少使用异常检测方法进行检测的概率，即 $1-p=\frac{\alpha}{\alpha+\beta}$ 会变小，这与我们的策略刚好相符。

当 β 一定时，α 越大，$p=q=\frac{\beta}{\alpha+\beta}$ 越小。同理，α 越大说明入侵检测系统中误用检测方法对常见攻击的检测率变大，这时攻击者应该尽量避免使用常见攻击方法对网络进行攻击，即 q 值减少，应多使用新型的攻击方法进行攻击；对防守者来说同理，这与我们的策略刚好相符。

当入侵检测系统中误用检测方法的检测率为 α，异常检测方法的检测率为 β 时，以 $(\frac{\beta}{\alpha+\beta},\frac{\alpha}{\alpha+\beta})$ 的概率使用误用检测方法和异常检测方法进行检测，可以使得入侵检测系统获取的收益最大，耗能更少。

2.2.3　多攻击检测博弈模型的实现

多攻击检测博弈模型将博弈论和现有的入侵检测模块整合起来，制定相应的防守策略，实现对多种入侵方式的检测，该模型的主要步骤如下：

步骤 1　初始化无线传感器网络，设置节点的基本信息，基站的基本信息。

步骤 2　使用网络分簇协议 LEACH 将网络划分为 k 个簇，基站根据簇的划分情况设置 $U(t),Avg,C_i(t),V_i(t),Q_i(t),P_i(t)$ 和 $W(t)$ 值的信息，这些值的含义如表 1 所列。

步骤 3 基站将这些值代入相应的公式中，构建出 $U_{ij}(D)$ 和 $U_{ij}(A)$，其中 $1\leqslant i,j\leqslant 2$。使用 $U_{ij}(D)$ 和 $U_{ij}(A)$ 构建出攻击者和防御者的收益矩阵 Y' 和 Z'。

步骤 4 基站对博弈双方的收益矩阵进行求解，判断其是否有纯策略纳什均衡。如果存在纯策略纳什均衡解，则求解出模型的解，执行步骤 7；否则执行步骤 5。

步骤 5 输入各模块的检测率 p 和 q。

步骤 6 根据 p 和 q 的值，结合上述公式构建出攻击者和防御者的混合收益 U_D 和 U_A，求解出博弈模型的混合纳什均衡解。

步骤 7 基站根据求出的解开启相应的检测模块，执行入侵检测过程，算法流程如图 1 所示。

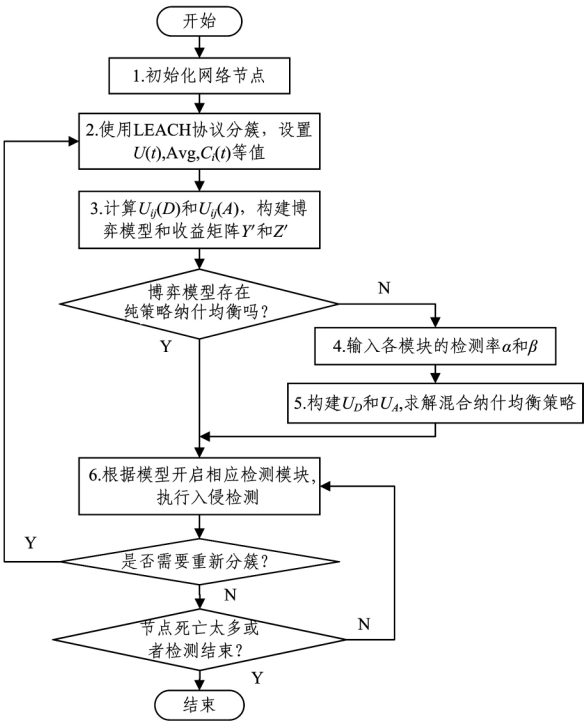

图 1 多攻击检测博弈模型流程图

3 仿真实验与分析

无线传感器网络属于大规模网络，目前传感器网络的网络应用的构建尚处于初始阶段，大规模的物理试验检测也难以实行。一定范围内的模拟仿真成为部分理论和技术方法验证的重要手段。本文提出的入侵检测系统策略构建于入侵检测模块之上，重点对节点的入侵检测的布局进行实验、配置，对底层的数据功能、采集处理等过程进行简化处理，为节省成本，我们选用了小米新出的温湿度传感器 2016DP0535，符合 ZiGBee 协议，该系统可以由小米手机相应的 App 管理控制，入侵则以信号干扰为主（人为调节），模拟实验在教学楼和部分室外场地进行，传感器 100 个、无线路由 5 个、小米手机 8 台，最后收集的各项数据再由 MATLAB 平台进行后续的模型理论处理与验证。

3.1 实验参数

在选定的 100m＊100m 传感区域中，随机部署了 100 个传感器节点，这些传感器节点的初始能量均设定为 0.5J，并且节点一旦部署完毕以后就不可移动，基站节点位于整个传感区域的中央且其能量不受限制。传感器节点使用 LEACH 分簇算法进行簇的划分。它的基本思想是通过随机循环地选举簇头节点，将整个网络的能量负载平均分配到每个传感器节点中，从而达到降低网络能源消耗、提高网络寿命的目的。虽然小米温湿度传感器的实际能耗不容易测量，但由于这些传感器都一样，因此可以将它们视为能量消耗相同，采用 LEACH 分簇算法进行簇的划分时可以在地理位置内均衡分布传感器来选择。由于节点被选举为簇头的概率为 0.1，因此整个网络中拥有 10 个簇头节点。仿真的参数如表 2 所列。

表 2 模拟实验参数表

参数	值	参数	值
检测区域大小/m	100×100	节点是否可运动	否
传感器节点数量	100	节点初始化能量/J	0.5
基站位置/m	(50,50)	发送或接受数据的单位能耗 E_{elec}(nJ/bit)	50
网络分簇协议	LEACH	自由空间信道模型发射放大器功耗参数 E_{fs} pJ/(bit×m^2)	10
节点选举为簇头的概率	0.1	多路径衰减信道模型发射放大器功耗参数 E_{mp} pJ/(bit×m^2)	0.013

图 2 为 MATLAB 仿真的网络结构图。在该图中，使用 LEACH 分簇协议选择的簇头节点用“＋”号表示，普通节点用实心点表示。基站使用星号表示，位于整张网络的中心位置，它可以向簇头节点发送控制信息。

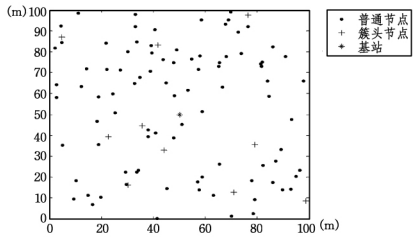

图 2 随机分布节点组成的簇状网络

在图 3 中，“＋”号点为网络攻击者进行攻击的时间点数据，“———”曲线为拟合后的曲线。

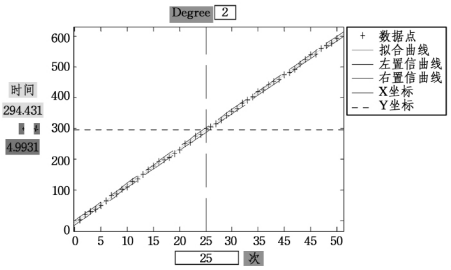

图 3 时间点曲线拟合图

由图 3 中 Degree 值可以看出，使用了二次曲线对其进行拟合。在拟合曲线的左右两边均有一条置信曲线，我们在 polytool 函数中传入的参数为 0.05，因此该曲线为 95％置信曲线，说明 95％的数据落在这两条线之间。本图中，该区间的大小为 4.9331，也就是说用预测值加减 4.9331 构成的时间区间，将以 95％的置信率包含真实的攻击时间点。

假设入侵检测系统中误用检测模块对常见攻击的检测率为 0.9，异常检测模块对新型攻击的检测率为 0.9，根据改进的博弈模型可以知道，入侵检测系统应以(0.5,0.5)的概率启动入侵检测模块，运行仿真实验。

为了使实验结果更具有说服力，在相同的条件下，引入了流量预测入侵检测算法和簇头监视入侵检测算法进行对比实验。流量预测入侵检测算法的基本思想是：在每次的入侵检测过程中，选择簇内流量最大的簇节点进行保护；簇头监视入

侵检测算法的基本思想是：在所有的簇头节点中均运行入侵检测系统。图 4 为在相同情况下，各个入侵检测算法的入侵检测率。

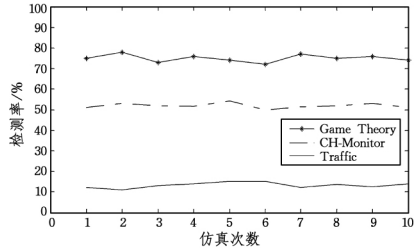

图 4　入侵检测率对比图

从图 4 中可以看出，使用博弈论对网络攻防过程进行建模后，能够使网络在应对多种网络攻击的情况下，仍然保持较高的检测率，相对稳定在 75%左右。使用簇头检测模型算法的入侵检测效率维持在 50%左右，这主要是因为在所有的簇头节点中运行入侵检测系统会较快地消耗系统能量，使得整体的入侵检测效率有所下降。由于没有方法来指定检测模块的启动顺序，因此只能以等概率的方式随机启动检测模块。根据现有文献的一般共识[6]，基于流量的入侵检测算法的入侵检测率维持在 15%左右，这主要是因为簇中流量的大小和攻击者的攻击选择之间没有必然的联系。

由此可以得出，使用博弈论的入侵检测算法能够以较高的检测率对多种攻击进行检测，这保证了 WSN 网络在更加复杂的网络环境下能够安全使用。

3.2　能耗评估

在使用仿真实验进行能耗评估之前，分析给出一个可对比的计算公式。假设无线传感器网络中有 N 个节点，需要在待监测区域中部署的总时间为 T，无线传感器中布置的入侵检测系统在单位节点中单位时间内的能量消耗为 μ。当入侵检测系统布置在全部的节点中并实时开启时，消耗的能量为 p_1，则：

$$p_1=\mu NT \tag{6}$$

当使用分簇算法将网络划分为 K 个簇，只在簇头中布置入侵检测系统并实时开启时，消耗能量为 p_2，则：

$$p_2=\mu KT \tag{7}$$

将时间 T 平均分为 n 个时间间隙，记为 $T_1,T_2,\cdots,T_N$。由于系统需要获取一定的历史数据用来预测攻击者后续的攻击行为。因此，在网络刚部署的一段时间 T' 内入侵检测系统是全部开启的。通过将时间 T' 内获取的历史数据应用到系统中后，可以计算出在置信概率为 $\alpha\%$ 下的攻击时间误差阈值 δ。本系统需要消耗的能量 p_3 为：

$$p_3=\mu(KT'+2\delta n(1-\frac{T'}{T})) \tag{8}$$

在本次仿真实验中，无线传感器网络中共有 $N=100$ 个节点，监测时间 $T=10\text{min}$，使用 LEACH 分簇算法时设置的簇头概率为 0.1，簇头节点共有 $K=100*0.1=10$ 个，使用本入侵检测系统时，将监测时间划分成了 $n=50$ 个间隙，取前 20 个间隙的入侵数据作为历史数据，通过对攻击者的入侵时间点进行拟合，得出置信曲线区间在 95%的置信率下包含真实入侵时间点的误差阈值为 $\delta=4.9331$，入侵检测节点在单个节点中单位时间内消耗的能量在 3 种情况下基本不变。将上述数值代入式(6)－式(8)中，并进行简单的计算可以得到：

$$\frac{p_2}{p_1}=0.1 \tag{9}$$

$$\frac{p_3}{p_2}=0.4491 \tag{10}$$

从上面的计算中可以看出，理想情况下，现有的基于簇的入侵检测算法与基于节点的入侵检测算法相比，能耗下降了 90%左右；本系统的入侵检测算法与现有的基于簇的检测算法相比，能耗下降了 55%左右。

在仿真实验中，我们对节点的能量消耗进行了记录，通过在每种情况下对 WSN 网络提供服务的时间进行对比，来评估系统的能量消耗，这是一个最直接的指标。图 5 为在相同情况下系统的能耗对比图。图中网络的可用性指的是网络可以用来提供相应的服务。在相同初始能量的情况下，网络的可用性越长，说明系统的能耗越低。

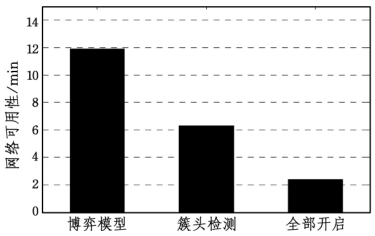

图 5　网络可用性对比图

两者之间的差值是因为在理想情况下，我们并没有考虑到引入簇划分协议所带来的额外的能量消耗，也没有考虑入侵检测系统防御攻击不成功时需要消耗的额外能量。

从图 5 中可以看出，在相同的实验环境下，使用博弈检测模型的无线传感器网络的可用性时长约是使用簇头检测的 2 倍，是节点全部开启时网络可用性时长的 5 倍左右。通过简单的计算可知，基于博弈的入侵检测系统与现有的簇头检测算法相比，能耗下降了大约 47%左右。

结束语　由于无线传感器网络存在巨大的应用价值，其入侵也随之扩散，国内外现有的入侵检测系统大多只对特定的攻击方式具有较高的检测率，对其他攻击则显得无能为力；入侵检测系统在保护系统安全的同时也增加了系统的能量消耗。本文以无线传感器网络中的入侵检测算法为研究重点，结合博弈理论，运用非合作完全信息静态博弈原理，构建了无线传感器网络中的入侵检测模型。通过模拟实验，新模型的有效性得到了验证。

博弈论方法也为无线传感器网络安全中多方面关键问题的研究提供了可行的新思路和新技术，这是一个重要的充满前景的研究方向，例如研究对特定攻击具有较高检测率的入侵检测算法与实际无线传感器网络环境的融合问题等。

致　谢　由于在模拟实验部分有 100 多个传感器、路由及手机，需要较多人力，因此感谢华科附中高级中学韩福济等近 20 多位同学近 3 周的参与付出。

参 考 文 献

[1] PERRIG A, STANKOVIC J, WAGNER D. Security in wireless sensor networks[J]. Communications of ACM, 2004, 47(6): 53-57.

[2] 裴庆祺，沈玉龙，马建峰. 无线传感器网络安全技术综述[J]. 通信学报，2007，28(8)：113-122.

[3] PING Y, HAO X J, YUE W, et al. Distributed intrusion detection for mobile ad hoc networks[J]. Journal of Systems Engi-

neering and Electronics,2008,19(4):851-859.
[4] LIAO H J,LIN C H R,LIN Y C,et al. Intrusion detection system:A comprehensive review[J]. Journal of Network and Computer Applications,2013,36(1):16-24.
[5] KAVITHA T,SRIDHARAN D. Security vulnerabilities in wireless sensor networks:A survey[J]. Journal of information Assurance and Security,2010,5(1):31-44.
[6] YAN K Q,WANG S C,LIU C W. A hybrid intrusion detection system of cluster based wireless sensor networks[C]// Proceeding of the International Multi Conference of Engineers and Computer Scientists. 2009,1:18-20.
[7] ALRAJEH N A,KHAN S,SHAMS B. Intrusion detection systems in wireless sensor networks:a review[J]. International Journal of Distributed Sensor Networks,2013,2013(1):113-120.
[8] GUTIERREZ J A,NAEVE M,CALLAWAY E,et al. IEEE 802.15.4:a developing standard for low-power low-cost wireless personal area networks[J]. Network,IEEE,2001,15(5):12-19.
[9] YICK J,MUKHERJEE B,GHOSAL D. Wireless sensor network survey[J]. Computer Networks,2008,52(12):2292-2330.
[10] AKYILDIZ I F,SU W,SANKARASUBRAMANIAM Y,et al. Wireless sensor networks:a survey[J]. Computer Networks,2002,38(4):393-422.
[11] AL-KARAKI J N,KAMAL A E. Routing techniques in wireless sensor networks:a survey[J]. Wireless communications,IEEE,2004,11(6):6-28.
[12] **李慧芳,姜胜明,韦刚. 无线传感器网络中基于博弈论的路由建模[J]. 传感器技术学报**,2007,20(9):1-3.

(**上接第** 293 **页**)

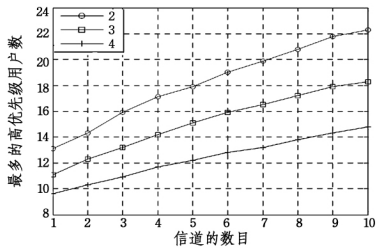

图 9 **最多的高优先级用户数图**

结束语 **本文提出了一种针对分布式认知无线电网络的** MAC **协议,该协议确保了时延敏感性应用的优先级高于普通用户。通过仿真分析表明,该协议降低了信道的接入时延,满足时延敏感性应用的** QoS **需求。本文还根据高优先级应用的** QoS **需求,提出了一种计算此类用户最大数量的方法,这可以用来改进信道的接入控制模块。通过数值分析进一步表明,本文提出的协议较其他同类协议具有较高的吞吐量。本文提出的** Q-MAC **协议还确保在数据传输阶段,次用户间不会发生冲突,这有效地提高了频谱空洞的利用率。并且,该协议不是通过增加次用户节点的复杂度,而是采用一种快速的控制信息交换机制,解决了隐藏终端的问题。因此,网络的初始化、重构和协调,甚至在不同频谱的可用性方面,**Q-MAC **协议均是易于实现且可信的。**

参 考 文 献

[1] CHENG Y C,WU E H,CHEN G H. A Decentralized MAC Protocol for Unfairness Problems in Coexistent Heterogeneous Cognitive Radio Networks Scenarios with Collision-Based Primary Users[J]. IEEE System Journal,2016,10(1):346-357.
[2] **杨劲松,曾碧卿,胡翩翩. 认知无线电网络中基于和声搜索的频谱分配与功率控制[J]. 计算机科学**,2015,42(11A):258-262.
[3] JOSHI G P,NAM S Y,KIM S W. Decentralized Predictive MAC Protocol for Ad Hoc Cognitive Radio Networks[J]. Wireless Personal Communications,2014,74(2):803-821.
[4] YUAN Y,BAHL P,CHANDRA R,et al. Allocating dynamic time-spectrum blocks in cognitive radio networks[J]. IEEE Transactions on Wireless Communications,2014,13(2),630-645.
[5] ZHU L,ZHOU H. Two Types of Attacks against Cognitive Radio Network MAC Protocols[C]// 2008 International Conference on Computer Science and Software Engineering. Wuhan:IEEE Press,2008:1110-1113.
[6] **夏海轮,许航天,丁炜. 移动** Ad hoc **网络中的** QoS **技术[J]. 中国科技论文在线**,2006,1(3):212-216.
[7] HU J,SHEN L F,SONG T C. QoS-based MAC protocol for cognitive radio networks[J]. Journal of Southeast Unicersity,2012,4(28):375-379.
[8] DE DOMENICO A,STRINATI E C,DI BENEDETTO M G. A survey on MAC strategies for cognitive radio networks[J]. IEEE Commun. Surveys & Tutorials,2012,14(1):21-44.
[9] SU H,ZHANG X. Cross-layer based opportunistic MAC protocols for QoS provisionings over cognitive radio wireless networks[J]. IEEE J. Sel. Areas Commun,2008,26(1):118-129.
[10] SONG H,LIN X. A group based MAC protocol for QoS provisioning in cognitive radio networks[C]// 11th IEEE Singapore International Conference on Communication Systems. Guangzhou:IEEE Press,2008:1489-1493.
[11] ZHAO Q,TONG L,SWAMI A,et al. Decentralized cognitive MAC for opportunistic spectrum access in ad hoc networks:a POMDP framework[J]. IEEE J. Sel. Areas Commun,2007,25(3):589-600.
[12] ZHANG Y,LAZOS L,CHEN K. FD-MMAC:Combating multi-channel hidden and exposed terminals using a single transceiver[C]// 2014 Proceedings IEEE INFOCOM. Toronto:IEEE Press,2014:2742-2750.
[13] JHA S C,RASHID M M,BHARGAVA V K,et al. Q-MAC:an opportunistic multichannel MAC for cognitive radio networks[C]// IEEE 70th Vehicular Technology Conference Fall (VTC 2009-Fall). Anchorage:IEEE Press,2009:1-5.
[14] BIANCHI G. Performance analysis of the IEEE 802.11 distributed coordination function[J]. IEEE J. Sel. Areas Commun,2000,18(3):535-547.
[15] ZIOUVA E,ANTONAKOPOULOS T. CSMA/CA performance under high traffic conditions:throughput and delay analysis[J]. Comput. Commun.,2002,25(3):313-321.
[16] MO J,SO H S,WALRAND J. Comparison of multichannel MAC protocols[J]. IEEE Trans. Mobile Comput.,2008,7(1):50-65.