# WSNs 多阶段入侵检测博弈最优策略研究

周伟伟* 郁 滨
(信息工程大学 郑州 450001)

**摘 要**：针对无线传感器网络中资源受限的入侵检测系统策略优化问题，该文提出一种多阶段动态入侵检测博弈模型。该模型利用贝叶斯规则修正下一阶段外部节点为恶意节点的后验概率，通过分析推导给出最易遭受攻击的节点集合。以建立的模型和节点集合为依据，求解了满足完美贝叶斯均衡条件的入侵检测最优策略。在此基础上，设计了入侵检测最优策略方案。仿真实验结果表明，该方案在提高簇形结构检测防御成功率方面有明显优势。

**关键词**：无线传感器网络；多阶段博弈；入侵检测；后验概率；贝叶斯均衡
**中图分类号**： TP393.08 **文献标识码**： A **文章编号**：1009-5896(2018)01-0063-09
**DOI**: 10.11999/JEIT170323

# Optimal Defense Strategy in WSNs Based on the Game of Multi-stage Intrusion Detection

ZHOU Weiwei YU Bin
(*Information Engineering University*, *Zhengzhou* 450001, *China*)

**Abstract**: To overcome the problem that the performance of intrusion detection deteriorates significantly in resource-constrained wireless sensor networks, a dynamically multi-stage game model of intrusion detection is proposed. Based on the Bayesian rules and prior probability that external node is a malicious node in this stage, the posterior probability of external node and the set of node vulnerable to attack are formulated respectively. Then, the optimal defense strategy for intrusion detection is calculated accurately according to the conditions of perfect Bayesian equilibrium. On this basis, a novel scheme for intrusion detection is proposed in WSNs based on the optimal strategy of multi-stage game model. Finally, experimental results show that the developed scheme has distinct advantage in improving the success rate of detection and suppression in clustered WSNs.

**Key words**: Wireless Sensor Networks (WSNs); Multi-stage game; Intrusion detection; Posterior probability; Bayesian equilibrium

## 1 引言

无线传感器网络(Wireless Sensor Networks, WSNs)节点高冗余度、低功耗、自组织以及部署速度快的特点使其在战场环境侦测、目标追踪、态势感知等领域有着广泛的应用前景[1]。但是，WSNs 在开放且带宽有限的无线信道中进行数据传输，极易遭受各种安全威胁。入侵检测作为一种积极主动的攻击防御技术，提供了防范内部攻击和外部攻击的能力[2–4]。目前，WSNs 入侵检测的研究主要包括检测模型和检测算法。

在检测模型方面，Kolias 等人[5]提出了基于簇头节点的分布式入侵检测系统，单点独立检测模型的检测功能由簇头节点实现，该模型提高检测率的同时增加了系统开销。Yu 等人[6]在分布式网络基础上利用簇头节点流量预测检测攻击节点，通过 ARMA 模型对网络各区域的数据流量进行线性预测建模，设置流量阈值来检测入侵节点。由于 ARMA 模型具有误报率高的特点，Patel 等人[7]提出了一种合作式入侵检测结构，当本地检测引擎无法确定时可以由邻居节点投票决定。Kalnoor 等人[8]构建了基于代理合作的入侵检测结构，通过监测代理、决策代理和执行代理对等合作实现对攻击节点的隔离，但该模型未考虑 WSNs 中不同层级节点的资源特性。基于此，文献[9]提出了层次式混合检测架构，依据不同功能节点的能力及所面临的威胁程度对可疑节点实施卡尔曼滤波，通过阈值判定节点的状态。

在检测算法方面，Forootaninia 等人[10]提出了合作式看门狗检测方法，由数据发送者和接收者的

收稿日期：2017-04-13；改回日期：2017-09-01；网络出版：2017-11-01
*通信作者：周伟伟 1099471246@qq.com
基金项目：信息保障重点实验室开放基金(KJ-15-104)，河南省科技攻关项目(132102210003)
Foundation Items: The National Science Key Laboratory Fund (KJ-15-104), The Project of Key Scientific and Technological Research of Henan Province (132102210003)

邻居节点作为看门狗监视测量参数与阈值之间的关系，通过轮换机制提高检测响应速度，但算法是在已知安全威胁类型的基础上，并不适用于未知网络环境。Doumit 等人[11]利用竞争聚类学习算法训练和修改监督规则，使网络容忍标签丢失，提高了系统的自学习功能，但有限的监督规则使系统鲁棒性较差。文献[12]提出卡方检测方法，利用正常数据样本点服从高斯分布的特性，判定数据样本与已知分布之间的似然估计值较小时为异常行为。Jokar 等人[13]采用支持向量机技术，通过测试样本的本地半径与全局半径阈值对比实现入侵检测，但该方法需要处理大量数据，计算复杂度大。为减小算法的计算开销，Moosavi 等人[14]提出了基于马尔可夫模型的异常行为检测机制，但阈值确定难度大，导致该算法检测准确率较低。

一方面，目前 WSNs 入侵检测的研究集中于检测抑制方案设计层面，但由于节点电源能量、通信能力以及计算能力有限等特点，各方案在系统中的实现需要适应节点有限资源特性，否则嵌入安全方案的部分节点能量迅速耗尽，威胁网络拓扑和系统安全。在资源有限的节点中运行入侵检测机制，保证通信安全的同时使资源利用达到最优，其本质是攻击者与持有多种安全策略的 WSNs 系统之间的最优化博弈问题。

本文通过分析对比不同策略集下外部节点的收益函数，得到 WSNs 簇形结构内具有攻击价值的传感器节点，利用贝叶斯规则求解不同阶段入侵检测系统持有的外部节点为恶意节点的后验概率，结合多阶段最优策略集设计入侵检测方案。最后，实验对比分析了本文方案与其它方案的入侵检测性能。

## 2 网络模型及参数分析

WSNs 簇形结构由一个簇头和固定数量的传感器节点构成。假设攻击节点和入侵检测系统均是理性的，其策略由收益函数支配。入侵检测系统和攻击节点的资源有限。一个或多个恶意节点攻击同一传感器节点时攻击收益相同。模型中的符号及其含义如表 1 所示。

### 2.1 模型构建

合法的信任节点包括簇头和协调器，外部节点类型可能是合法的或恶意的，恶意节点可以攻击簇内所有传感器节点。入侵检测系统由簇头节点与簇内传感器节点相互配合实现对恶意节点的防御，网络模型如图 1 所示。外部节点与 WSNs 入侵检测系统之间的博弈过程可以用信号博弈来描述，将连续时间分割成独立的时间槽，每个时间槽内完成一次信号博弈，在连续时间内构成多阶段动态入侵检测博弈。

**表 1 所用符号含义表**

| 符号 | 含义 | 符号 | 含义 |
|---|---|---|---|
| $p_i$ | 攻击传感器节点 $i$ 的概率 | $q_i$ | 对节点 $i$ 实施检测防御的概率 |
| $C_0$ | 外部节点与簇内节点合作 | $A_0$ | 外部节点攻击簇内节点 |
| $P$ | 外部节点的资源约束 | $Q$ | 入侵检测系统的资源约束 |
| $W_i$ | 簇内传感器节点 $i$ 的安全权值 | $\Gamma$ | 可能被攻击的传感器节点集合 |
| $p_i^*$ | 攻击传感器节点 $i$ 的均衡解 | $q_i^*$ | 检测传感器节点 $i$ 的均衡解 |
| $a$ | 检测成功率 | $b$ | 误报率 |
| $D_0$ | 簇内节点采取防御动作 | $I_0$ | 簇内节点采取闲置动作 |
| $C_aW_i$ | 攻击节点 $i$ 的资源消耗 | $C_dW_i$ | 节点 $i$ 防御攻击的资源消耗 |
| $C_fW_i$ | 误报产生的资源消耗 | $\Theta$ | 参与者的类型空间 |
| $\beta$ | 无线信道的可靠度 | $P^{(t)}(\theta_S=1)$ | $t$ 阶段外部节点为恶意节点的后验概率 |

**定义 1** 多阶段动态入侵检测博弈 $G$ 是一个七元组 $\mathbb{Z}(N,\Theta,A,P_E,P_A,Q_D,U)$，其中：

(1) $N=\{$外部节点 $S$，入侵检测系统 $R\}$是一个包含两个参与者的集合；

(2) $\Theta=\Theta_S\times\Theta_R$，其中 $\Theta_S=\{\theta_S=0,\theta_S=1\}$ 是 $S$ 的类型空间，分别表示 $S$ 为合法节点和恶意节点，$\Theta_R=\{\theta_R=1\}$ 是 $R$ 的类型空间；

(3) $A=A_S\times A_R$，其中 $A_S=\{\{a_S(\theta_S=0)\,|\,C_0\},\{a_S(\theta_S=1)\,|\,A_0,C_0\}\}$ 是 $S$ 可采取的动作集合，$A_R=\{a_R\,|\,D_0,I_0\}$ 是 $R$ 可采取的动作集合；

(4) $P_E:\Theta_S\mapsto[0,1]$ 是 $S$ 的先验概率，$P=(p,1-p)$，其中 $p$ 表示恶意节点的概率；

(5) $P_A=(p_1,p_2,\cdots,p_N)$ 表示 $S$ 攻击簇内 $N$ 个正常成员传感器节点的概率；

(6) $Q_D=(q_1,q_2,\cdots,q_N)$ 表示 $R$ 中簇头在 $N$ 个正常成员传感器节点上实施检测防御的概率；

(7) $U=(u_S,u_R)$，其中，$u_S$ 是外部节点的支付函数，$u_R$ 是入侵检测系统的支付函数。

簇内传感器节点集合为 $\Gamma=\{1,2,\cdots,N\}$，安全权值集合为 $W=\{W_1,W_2,\cdots,W_N\}$，且 $W_1\geq W_2\geq\cdots$

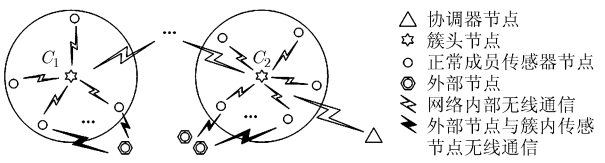



图 1 WSNs 入侵检测网络模型

$\geq W_N$。假设簇形结构中的资源满足 $\sum_{i\in\Gamma} p_i \leq P$，$\sum_{i\in\Gamma} q_i \leq Q \leq 1$。$S$ 为合法节点和恶意节点的支付矩阵如表 2 所示。

**表 2 阶段入侵检测博弈的支付矩阵**

**(a)外部节点 $S$ 是合法节点**

| | $D_0$ | $I_0$ |
|---|---|---|
| $C_0$ | $0,-bC_fW_i-C_dW_i$ | 0,0 |

**(b)外部节点 $S$ 是恶意节点**

| | $D_0$ | $I_0$ |
|---|---|---|
| $A_0$ | $(1-\beta)W_i+\beta(1-2a)W_i-C_aW_i$, $-(1-\beta)W_i-\beta(1-2a)W_i-C_dW_i$ | $W_i-C_aW_i,-W_i$ |
| $C_0$ | $0,-bC_fW_i-C_dW_i$ | 0,0 |

设第 1 阶段博弈中 $S$ 为恶意节点的先验概率为 $p$，依据贝叶斯规则，簇头可以从 $t$+1 阶段博弈结束时更新得到 $S$ 为恶意节点的后验概率，可表示为

$$P^{(t+1)}\left(\theta_S=1\mid\hat{a}_S(t+1)\right)=\frac{P\left(\hat{a}_S(t+1)\mid\theta_S=1\right)\cdot P^{(t)}\left(\theta_S=1\mid\hat{a}_S(t)\right)}{\sum_{\bar{\theta}_S\in\Theta_S}P\left(\hat{a}_S(t+1)\mid\bar{\theta}_S\right)\cdot P^{(t)}\left(\bar{\theta}_S\mid\hat{a}_S(t)\right)}\quad(1)$$

其中，$\hat{a}_S(t)$ 表示 $R$ 在 $t$ 阶段判断 $S$ 所采取的动作，$\hat{a}_S(t)$ 与 $a_S(t)$ 的差异性由 $a$ 和 $b$ 决定。$P^{(t)}(\theta_S=1\mid\hat{a}_S(t))$ 为 $t$+1 阶段 $S$ 为恶意节点的先验推断，$P(\hat{a}_S(t+1)\mid\theta_S=1)$ 表示 $t$+1 阶段 $S$ 为恶意节点时 $R$ 判定动作为 $\hat{a}_S(t+1)$ 的概率。设 $\theta_S=1$ 时恶意节点执行 $A_0$ 和 $C_0$ 的混合策略为 $\delta_S=(\rho,1-\rho)$，则有 $\rho=\sum_{i\in\Gamma}p_i$。

式(1)中各概率公式可表示为

$$P\left(\hat{a}_S(t+1)=A_0\mid\theta_S=1\right)=a\rho\beta+(1-\rho)\cdot b\beta\quad(2)$$

$$P\left(\hat{a}_S(t+1)=A_0\mid\theta_S=0\right)=b\beta\quad(3)$$

$$P\left(\hat{a}_S(t+1)=C_0\mid\theta_S=1\right)=1-\beta+(1-a)\cdot\rho\beta+(1-b)\cdot(1-\rho)\beta\quad(4)$$

$$P\left(\hat{a}_S(t+1)=C_0\mid\theta_S=0\right)=1-b\beta\quad(5)$$

随着 $P^{(t)}$ 的更新，博弈模型 $G$ 存在完美贝叶斯均衡必须满足贝叶斯条件[11]。

**定义 2**　贝叶斯条件包括：

(1)先验概率到后验概率的更新通过贝叶斯规则实现；

(2)各参与者的后验概率是相互独立的，并且参与者的所有类型具有同一个先验概率；

(3)参与者不传递任何参与者所不知道的事件信号；

(4)后验概率在 $\Theta$ 上的共同联合概率分布是一致的。

**定理 1**　如果多阶段动态入侵检测博弈定义在 $G$ 上，那么该博弈满足贝叶斯条件。

**证明**　后验概率的求解由式(1)得到，贝叶斯条件(1)满足。由于 $R$ 只有检测防御功能，贝叶斯条件(2)满足。$S$ 的信号由执行动作决定，若 $a_S(t)=a_S'(t)$，$P\left(\theta_S\mid a_S(t)\right)=P\left(\theta_S\mid a_S'(t)\right)$，贝叶斯条件(3)满足。每一个博弈阶段只有两个参与者，其它节点不影响 $S$ 是否为恶意节点的后验概率更新，贝叶斯条件(4)满足。　证毕

利用 $S$ 的支付矩阵和后验概率 $P^{(t)}$，可得外部节点和入侵检测系统的收益函数为

$$u_S\left(P_A,Q_D\right)=P^{(t)}\cdot\sum_{i\in\Gamma}p_iW_i\left(1-2a\beta q_i-C_a\right)\quad(6)$$

$$u_R\left(P_A,Q_D\right)=\sum_{i\in\Gamma}q_iW_i\left[p_i\cdot P^{(t)}\left(2a\beta+bC_f\right)-\left(bC_f+C_d\right)\right]-P^{(t)}\cdot\sum_{i\in\Gamma}p_iW_i\quad(7)$$

由于攻击者具有有限资源且节点具有不同安全权值，如何确定易受攻击节点集合是求解 $p_i^*$ 和 $q_i^*$ 的关键。

### 2.2 节点安全权值分析

为了研究攻击者对不同安全权值传感器节点的攻击特点，依据安全权值划分不同的传感器节点集合。

**定义 3**　最易遭受攻击的节点集合 $\Gamma_S$ 和较易遭受攻击的节点集合 $\Gamma_Q$ 满足式(8)条件：

$$\left.\begin{aligned}&W_i>\eta,\ \ \forall i\in\Gamma_S\\&W_i=\eta,\ \ \forall i\in\Gamma_Q\\&W_i<\eta,\ \ \forall i\in\Gamma-\Gamma_S-\Gamma_Q\end{aligned}\right\}\quad(8)$$

其中，$|\Gamma_S|$ 是集合 $\Gamma_S$ 的基数，$\Gamma-\Gamma_S-\Gamma_Q$ 表示节点 $i$ 既不属于集合 $\Gamma_S$ 又不属于集合 $\Gamma_Q$，

$$\eta=\frac{|\Gamma_S|\cdot(1-C_a)-2a\beta Q}{\left(\sum_{j\in T_S}\frac{1}{W_j}\right)(1-C_a)}$$

**引理 1**　WSNs 簇形结构中，若传感器节点持有不等的安全权值，那么集合 $\Gamma_S$ 和 $\Gamma_Q$ 具有唯一性，$\Gamma_S$ 由 $N_A$ 个具有最高安全权值的传感器节点组成，满足结论：

(1) 如果 $W_N>(N(1-C_a)-2a\beta Q)/(1-C_a)\cdot\sum_{j=1}^{N}\frac{1}{W_j}$，则 $N_A=N$，$\Gamma_S=\Gamma$，$\Gamma_Q=\varnothing$。

(2) 如果 $W_N\leq(N(1-C_a)-2a\beta Q)/(1-C_a)\cdot\sum_{j=1}^{N}\frac{1}{W_j}$，则 $N_A$ 由式(9)确定：

$$W_{N_A}>\frac{N_A\cdot(1-C_a)-2a\beta Q}{\left(\sum_{j=1}^{N_A}\frac{1}{W_j}\right)\cdot(1-C_a)}\geq W_{N_A+1} \tag{9}$$

**证明** 结论(1)中，当$W_N>(N(1-C_a)-2a\beta Q)/(1-C_a)\sum_{j=1}^{N}\frac{1}{W_j}$时，对$\forall i<N$，有$W_i\geq W_N$，显然满足$W_i>\frac{N\cdot(1-C_a)-2a\beta Q}{\left(\sum_{j\in T_S}\frac{1}{W_j}\right)(1-C_a)}$，由此可得，$N_A=N,\Gamma_S=\Gamma,\Gamma_Q=\varnothing$。结论(1)得证。

结论(2)中，要证明$N_A$存在并满足式(9)必须进行存在性和唯一性证明。

(a)存在性证明：由于$W_N\leq(N(1-C_a)-2a\beta Q)/(1-C_a)\sum_{j=1}^{N}\frac{1}{W_j}$，因此$N_A<N$。由式(9)得$W_{N_A+1}\cdot\left(\sum_{j=1}^{N_A+1}\frac{1}{W_j}\right)\cdot(1-C_a)\leq(N_A+1)\cdot(1-C_a)-2a\beta Q$。$N_A$个权值最高的节点集合满足式(8)中$\Gamma_S$的条件约束。

(b)唯一性证明：假设$\Gamma_S$中存在$m$个节点构成集合的情况，且$m<N_A$。由式(9)可得，$W_{N_A}\left(\sum_{j=1}^{N_A}\frac{1}{W_j}\right)-(N_A-m)>m-\frac{2a\beta Q}{1-C_a}$。由于$m<N_A$，则有$W_{m+1}\geq W_{N_A}$。故可得$W_{m+1}>\frac{m\cdot(1-C_a)-2a\beta Q}{(1-C_a)\left(\sum_{j=1}^{m}\frac{1}{W_j}\right)}$。与定义3结论矛盾。同理可得$m>N_A$不成立。综上，引理1得证。

**定理 2** 在 WSNs 簇形结构中，如果一个攻击者是理性的，那么该攻击者不会攻击集合$\Gamma-\Gamma_S-\Gamma_Q$中的任何一个传感器节点。

**证明** 当$W_N>(N(1-C_a)-2a\beta Q)/(1-C_a)\cdot\left(\sum_{j=1}^{N}\frac{1}{W_j}\right)$时，$\Gamma-\Gamma_S-\Gamma_Q=\varnothing$。定理显然成立。

当$W_N\leq(N(1-C_a)-2a\beta Q)/(1-C_a)\left(\sum_{j=1}^{N}\frac{1}{W_j}\right)$时，构造向量$\boldsymbol{Q}_D^1=\left(q_1^1,q_2^1,\cdots,q_N^1\right)$，其分布情况如下所示。

$$q_i^1=\begin{cases}\left\{1-C_a-\left[N_A\cdot(1-C_a)-2a\beta Q\right]/W_i\right\}\cdot\sum_{j=1}^{N_A}\frac{1}{W_j}\Big\}\Big/2a\beta, & i\in\Gamma_S\\ 0, & i\in\Gamma-\Gamma_S\end{cases} \tag{10}$$

由式(10)可知，$q_i^1\geq 0$且$\sum_{i=1}^{N_A}q_i^1=Q$。设$R$的防御策略集为$Q_D=(q_1,q_2,\cdots,q_N)$，$\sum_{i=1}^{N_A}q_i\leq Q$，依据鸽巢原理，$\Gamma_S$中至少存在一个传感器节点$n$上的防御策略满足关系$q_n^1\geq q_n$。

假设理性攻击者会攻击$\Gamma-\Gamma_S-\Gamma_Q$中至少一个传感器节点，攻击策略为$P_A=(p_1,p_2,\cdots,p_N)$，满足$\sum_{i\in\Gamma-\Gamma_S-\Gamma_Q}p_i>0$。构造另一个攻击策略$P_A^1=\left(p_1^1,p_2^1,\cdots,p_N^1\right)$，其分布情况如式(11)所示。

$$p_i^1=\begin{cases}p_i, & i\in\Gamma_S,\ i\neq n\\ p_n+\sum_{i\in\Gamma-\Gamma_S-\Gamma_Q}p_j, & i=n\\ p_i, & i\in\Gamma_Q\\ 0, & i\in\Gamma-\Gamma_S-\Gamma_Q\end{cases} \tag{11}$$

分别计算$S$执行策略$P_A$和策略$P_A^1$的收益函数，理性攻击者选择收益函数较大的策略。结合式(6)、式(10)、式(11)及$q_n^1\geq q_n$可得$u_S(P_A,Q_D)-u_S\left(P_A^1,Q_D\right)<0$。综上，定理2得证。

## 3 博弈模型的求解

本节以外部节点$S$和入侵检测系统$R$的收益函数最优为求解依据，通过分组讨论参数取值范围以及博弈中消耗恶意节点与入侵检测系统的资源情况，实现对多阶段入侵检测博弈模型的求解。

**定理 3** 在 WSNs 簇形结构中，设$S$和$R$之间的多阶段入侵检测博弈均衡解为$\left(P_A^*,Q_D^*\right)$，则有

(1)如果$N_D\geq N_A$且$N_A(1-C_a)\geq 2a\beta Q$，那么

$$p_i^*=\begin{cases}H, & i\in\Gamma_S\\ \in[0,H], & i\in\Gamma_Q\\ =0, & i\in\Gamma-\Gamma_S-\Gamma_Q\end{cases}$$

$$q_i^*=\begin{cases}\frac{1}{2a\beta}\left(1-C_a-\frac{N_A(1-C_a)-2a\beta Q}{W_i\sum_{j=1}^{N_A}\frac{1}{W_j}}\right), & i\in\Gamma_S\\ =0, & i\in\Gamma-\Gamma_S\end{cases}$$

其中，$P_A$为$S$在$\Gamma_S$中分配的攻击概率总和，

$$H=\frac{P_A}{W_i\sum_{j=1}^{N_A}\frac{1}{W_j}}-\frac{bC_f+C_d}{P^{(t)}\cdot\left(2a\beta+bC_f\right)}\left(\frac{N_A}{W_i\sum_{j=1}^{N_A}\frac{1}{W_j}}-1\right),$$

$$\sum_{i\in\Gamma}p_i^*=P,\ \sum_{i\in\Gamma}q_i^*=Q,\ P_A>\left(N_A-W_{N_A}\sum_{j=1}^{N_A}\left(\frac{1}{W_j}\right)\right)\cdot\left(\left(bC_f+C_d\right)\Big/\left(P^{(t)}\left(2a\beta+bC_f\right)\right)\right)$$

(2)如果$N_D<N_A$，那么

$$p_i^*\begin{cases}=L, & W_i>W_{N_D+1}\\ \in[0,L], & W_i=W_{N_D+1}\\ =0, & W_i<W_{N_D+1}\end{cases}$$

$$q_i^*=\begin{cases}\dfrac{1+C_a}{2a\beta}\left(1-\dfrac{W_{N_D+1}}{W_i}\right), & W_i>W_{N_D+1}\\ =0, & W_i<W_{N_D+1}\end{cases}$$

其中，

$$\sum_{i\in\Gamma}p_i^*=P,\ \sum_{i\in\Gamma}q_i^*<Q,\ L=\frac{bC_f+C_d}{P^{(t)}\cdot\left(2a\beta+bC_f\right)}$$

(3)如果 $N_D\ge N_A$ 且 $N(1-C_a)<2a\beta Q$，那么

$$\begin{cases}p_i^*=\left(bC_f+C_d\right)\Big/P^{(t)}\left(2a\beta+bC_f\right)\\ q_i^*=\left(1-C_a\right)\Big/2a\beta\end{cases},\quad i\in\Gamma$$

其中，$\begin{cases}\sum_{i\in\Gamma}p_i^*<P\\ \sum_{i\in\Gamma}q_i^*<Q\end{cases}$。

**证明**　$\left(P_A^*,Q_D^*\right)$ 为博弈的贝叶斯均衡解，当 $P^{(t)}\cdot\sum_{i\in\Gamma}W_i\left(1-2a\beta q_i-C_a\right)<0$ 时，$p_i^*$ 将趋于 0；当 $0\le P^{(t)}\cdot\sum_{i\in\Gamma}W_i\left(1-2a\beta q_i-C_a\right)<P^{(t)}\cdot\sum_{j\in\Gamma}W_j\cdot\left(1-2a\beta q_j-C_a\right)$ 时，攻击者为提高收益选择减小 $p_i^*$ 的同时增加 $p_j^*$ 的值，将 $p_i^*$ 的值设定为 0。因此，由 $S$ 的收益函数 $u_S(P_A,Q_D)$ 可得：

$$\left.\begin{aligned}&0\le P^{(t)}\cdot\sum_{i\in\Gamma}W_i\left(1-2a\beta q_i-C_a\right)\\&\quad=P^{(t)}\cdot\sum_{j\in\Gamma}W_j\left(1-2a\beta q_j-C_a\right)\\&P^{(t)}\cdot\sum_{k\in\Gamma}W_k\left(1-2a\beta q_k-C_a\right)\le P^{(t)}\\&\quad\cdot\sum_{i\in\Gamma}W_i\left(1-2a\beta q_i-C_a\right)\\&\forall i,j,k\in\Gamma,\ p_i^*,p_j^*>0,\ p_k^*=0\end{aligned}\right\}\tag{12}$$

同理，由 $R$ 的收益函数 $u_R(P_A,Q_D)$ 可得：

$$\left.\begin{aligned}&0\le W_i\left[p_i\cdot P^{(t)}\left(2a\beta+bC_f\right)-\left(bC_f+C_d\right)\right]\\&\quad=W_j\left[p_j\cdot P^{(t)}\left(2a\beta+bC_f\right)-\left(bC_f+C_d\right)\right]\\&W_k\left[p_k\cdot P^{(t)}\left(2a\beta+bC_f\right)-\left(bC_f+C_d\right)\right]\\&\quad\le W_i\left[p_i\cdot P^{(t)}\left(2a\beta+bC_f\right)-\left(bC_f+C_d\right)\right]\\&\forall i,j,k\in\Gamma,\ q_i^*,q_j^*>0,\ q_k^*=0\end{aligned}\right\}\tag{13}$$

(1)当博弈结束时，$S$ 和 $R$ 的资源同时耗尽，即 $\sum_{i\in\Gamma}p_i^*=P,\sum_{i\in\Gamma}q_i^*=Q$。由式(12)和式(13)可得定理 3 中(1)的均衡解 $p_i^*$ 和 $q_i^*$。存在贝叶斯均衡解的必要条件为 $N_D\ge N_A$ 和 $N_A\left(1-C_a\right)\ge 2a\beta Q$。其中，$N_D=\left\lfloor\left(2a\beta+bC_f\right)P\Big/\left(bC_f+C_d\right)\right\rfloor$，$P_A$ 为恶意节点在 $\Gamma_S$ 中分配的攻击概率总和，且 $P_A>\left(N_A-W_{N_A}\cdot\sum_{j=1}^{N_A}\left(1/W_j\right)\right)\left(\left(bC_f+C_d\right)\Big/\left(P^{(t)}\left(2a\beta+bC_f\right)\right)\right)$。

(2)当博弈结束时，$S$ 资源耗尽而 $R$ 的资源未耗尽，即 $\sum_{i\in\Gamma}p_i^*=P$，$\sum_{i\in\Gamma}q_i^*<Q$。由 $u_R\left(P_A,Q_D\right)$ 可知，对于 $\forall i,j\in\Gamma,q_i^*>0$，$W_i\left[p_i\cdot P^{(t)}\left(2a\beta+bC_f\right)-\left(bC_f+C_d\right)\right]=0$，否则 $R$ 将利用剩余的资源增加 $q_i^*$ 使其收益提高。由式(12)和式(13)可得定理 3 中(2)的均衡解 $p_i^*$ 和 $q_i^*$。其中，由式(9)可得存在贝叶斯均衡的必要条件为 $N_D<N_A$。

(3)当博弈结束时，$S$ 和 $R$ 的资源均未耗尽，即 $\sum_{i\in\Gamma}p_i^*<P$，$\sum_{i\in\Gamma}q_i^*<Q$。由式(6)和式(7)可得定理 3 中(3)的均衡解 $p_i^*$ 和 $q_i^*$。由引理 1 可得存在贝叶斯均衡的必要条件为 $N_D\ge N_A$ 且 $N(1-C_a)\le 2a\beta Q$。

综上，定理 3 证毕。

**推论 1**　在定理 3 中，对 $\forall P_A'\ne P_A^*$，$\forall Q_D'\ne Q_D^*$，如果 $\widehat{P}_A=\arg\max_{\widehat{P}_A\in P_A}u_S\left(P_A,Q_D'\right)$ 且 $\widehat{Q}_D=\arg\max_{\widehat{Q}_D\in Q_D}u_S\left(P_A',Q_D\right)$，那么 $u_S\left(P_A^*,Q_D^*\right)>u_S\left(\widehat{P}_A,Q_D'\right)$，$u_S\left(P_A^*,Q_D^*\right)>u_S\left(P_A',\widehat{Q}_D\right)$。

**证明**　该推论的证明与定理 2 相似。

## 4　入侵检测最优策略设计

依据博弈的完美贝叶斯均衡解及各变量参数，设计适应于 WSNs 的入侵检测机制。该检测机制主要包括 4 个部分：参数存储模块、WSNs 安全管理中心、入侵检测系统 $R$、以及外部节点 $S$。各部分之间的交互关系如图 2 所示。WSNs 安全管理中心主要负责通过协调器向各簇头节点下发针对不同攻击的入侵检测机制。由于 WSNs 节点具有有限资源特性，在整个入侵检测多阶段博弈中，入侵检测系统资源在每个博弈阶段能够执行防御策略的总概率为 $Q$。在此基础上调整防御机制使入侵检测的策略收益达到最优。

当 $R$ 开启时，簇头节点开始初始化参数 $a$, $b$, $C_a$, $C_d$, $C_f$, $\delta_S$, $P^{(t)}\left(\theta_S=1\mid\hat{a}_S(t)\right)$, $p$。由于 $S$ 可能为恶意或者合法节点，因此 $S$ 可能采取动作 $A_0$ 或者 $C_0$，$R$ 中簇头节点通过监测 $S$ 得到最初的先验概率 $p$。依据不同节点采集数据的安全权值 $W_i$，$R$ 计算式(8)中执行防御策略的临界值。当节点的安全权值小于该临界值时，$R$ 实施防御的收益小于支付的成本，由

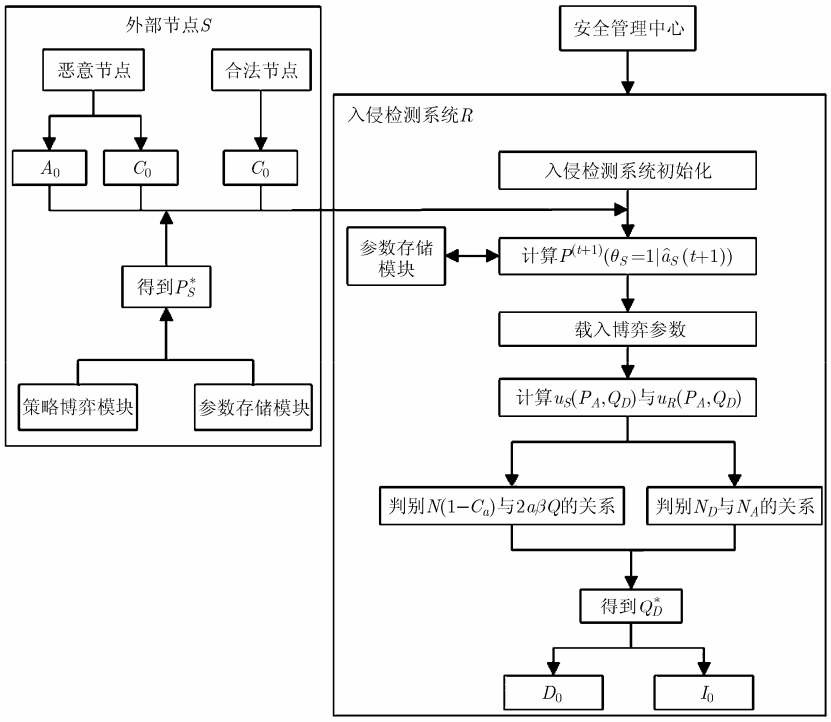



图2 基于完美贝叶斯均衡的入侵检测机制

引理 1 确定执行入侵检测防御的节点集合 $\Gamma_S+\Gamma_Q$。$R$ 的参数存储模块调用参数 $a$, $b$，依据式(2)~式(5)计算 $P(\hat{a}_S(t+1)\,|\,\theta_S=1)$，$P^{(t)}(\theta_S=1\,|\,\hat{a}_S(t))$ 和 $\sum_{\bar{\theta}_S\in\Theta_S}P\left(\hat{a}_S(t+1)\middle|\bar{\theta}_S\right)\cdot P^{(t)}\left(\bar{\theta}_S\middle|\hat{a}_S(t)\right)$，采用贝叶斯规则更新第 $t+1$ 阶段 $S$ 为恶意节点的后验概率 $P^{(t+1)}\left(\theta_S=1\middle|\hat{a}_S(t+1)\right)$。簇头节点载入博弈参数计算收益函数 $u_S\left(P_A,Q_D\right)$ 和 $u_R\left(P_A,Q_D\right)$。

$R$ 判别 $N\left(1-C_a\right)$ 与 $2a\beta Q$，$N_D$ 与 $N_A$ 之间的关系确定满足定理 3 中何种最优策略的必要条件，并利用 $P^{(t+1)}\left(\theta_S=1\middle|\hat{a}_S(t+1)\right)$, $u_S\left(P_A,Q_D\right)$, $u_R\left(P_A,Q_D\right)$ 求解入侵检测系统最优策略集 $Q_D^*$。由簇头分配与各传感器节点相结合的入侵检测资源，簇头以不同的概率与传感器节点共同实现对外部节点攻击的防御。

当 $S$ 启动最优策略攻击机制时，利用入侵检测系统持有的外部节点为恶意节点的先验概率 $p$ 以及贝叶斯规则得到 $S$ 为恶意节点的后验概率 $P^{(t+1)}\left(\theta_S=1\middle|\hat{a}_S(t+1)\right)$。通过计算 $S$ 和 $R$ 的收益函数并判别 $N\left(1-C_a\right)$ 与 $2a\beta Q$，$N_D$ 与 $N_A$ 之间的关系，由定理 3 确定满足何种最优策略的必要条件，使 $S$ 在有限资源 $P$ 的条件下收益最大，得到均衡解 $P_S^*$。$S$ 依据 $P_S^*$ 配置各博弈阶段的攻击策略。

## 5 实验与结果分析

为了验证本文提出模型的性能，利用 NS-2 配置网络参数及变量对模型进行仿真。实验中引入 3 种实验场景：(1)加载多阶段入侵检测博弈的安全协议；(2)引入文献[13]中基于支持向量机的入侵检测安全协议；(3)采用文献[14]中基于马尔可夫模型的入侵检测安全协议。具体实验参数如表 3 所示。

簇内节点的安全权值满足 $W_i=70-(i-1)\times 5$，$Q=1$ 且同一簇形结构仅有一个外部节点，即 $P=1$。

在表 3 配置的实验环境下，运行本文方案、文献[13]、文献[14]的入侵检测策略，得到第 15 个博弈阶段策略取值及收益函数如表 4 和表 5 所示。其中，策略取值和收益函数为 40 个簇形结构测量结果的均值。

从表 4 和表 5 可以看出，无论是第 15 个博弈阶段的入侵检测收益 $u_R$ 还是平均收益 $\bar{u}_R$，本文方案均明显优于文献[13]和文献[14]。本文方案依据节点安全权值和恶意节点后验概率调整和配置最优策略，而文献[13]和文献[14]未考虑外部节点为恶意节点的概率更新问题。

在表 4 中，随着传感器节点安全权值的减小，入侵检测系统分配给该节点的安全防御策略值减小。外部节点攻击传感器节点的策略值则随着节点安全权值的减小而增大。这是由于攻击缺乏安全策略保护的节点可以获得更大的收益。但从第 9 个传感器节点开始，攻击策略和防御策略均为 0，这是由于第 9~12 个节点在 $\Gamma-\Gamma_S-\Gamma_Q$ 中，攻击收益小

**表 3　NS-2 参数设置**

| | | | |
|---|---|---|---|
| 传感器节点初始能量 | 2 J | 单次博弈阶段时间(min) | 10 |
| 入侵攻击资源消耗系数 | $C_a = 0.3$ | 阶段博弈个数(个) | 15 |
| 入侵检测资源消耗系数 | $C_d = 0.2$ | 仿真区域($m^2$) | $200 \times 200$ |
| 误报的资源消耗系数 | $C_f = 0.01$ | 簇形结构数量(个) | 40 |
| 检测率 | $a = 0.9$ | 各簇形结构中节点数量(个) | 12 |
| 误报率 | $b = 0.06$ | 通信协议 | IEEE 802.15.4 |
| $S$ 为恶意节点的先验概率 | $p$=0.6 | 单个节点通信距离(m) | 65 |
| 信道可靠度 | $\beta = 0.95$ | 数据包大小(B) | 512 |
| 传感器节点初始能量 | 2 J | 入侵攻击形式 | Wormhole |
| 入侵攻击资源消耗系数 | $C_a = 0.3$ | 数据退避机制 | CSMA/CA |
| 协调器主机端内存 | 4 G | 簇头初始能量 | 5 J |

**表 4 入侵检测均衡策略**

| | 本文方案 | 文献[13]的方案 | 文献[14]的方案 |
|---|---|---|---|
| 最优策略 | $p_1^* = 0.092,\ q_1^* = 0.289$<br>$p_2^* = 0.103,\ q_2^* = 0.253$<br>$p_3^* = 0.114,\ q_3^* = 0.176$<br>$p_4^* = 0.126,\ q_4^* = 0.105$<br>$p_5^* = 0.131,\ q_5^* = 0.065$<br>$p_6^* = 0.139,\ q_6^* = 0.043$<br>$p_7^* = 0.142,\ q_7^* = 0.042$<br>$p_8^* = 0.153,\ q_8^* = 0.027$<br>$p_9^* = 0,\ q_9^* = 0$<br>$p_{10}^* = 0,\ q_{10}^* = 0$<br>$p_{11}^* = 0,\ q_{11}^* = 0$<br>$p_{12}^* = 0,\ q_{12}^* = 0$ | $p^* = 0.416,\ q^* = 0.509$ | $p^* = 0.373,\ q^* = 0.617$ |
| 收益函数 | $u_S = 0.754,\ u_R = -0.756$ | $u_S = 0.812,\ u_R = -0.815$ | $u_S = 0.837,\ u_R = -0.841$ |

**表 5 各博弈阶段的收益函数值**

| | 本文方案 | 文献[13]的方案 | 文献[14]的方案 |
|---|---|---|---|
| $(u_R)_{\max}$ | −0.756 | −0.815 | −0.841 |
| $\overline{u}_R$ | −0.826 | −0.852 | −0.879 |
| $(u_R)_{\min}$ | −0.931 | −0.961 | −0.987 |

于攻击成本。

当每个簇形结构内传感器节点个数 $N = 12$ 时，博弈阶段 $t$ 和成功对外部节点实施检测防御的簇形结构的个数 $M$ 之间的关系如图 3 所示。

在博弈开始阶段文献[13]的方案在所有簇形结构中检测成功的数量最多，而文献[14]和本文方案检测效果相当，这是由于文献[13]的方案采用了基于支持向量机的策略集，提高了簇头与多个传感器节点相配合检测恶意节点的概率。由于文献[14]在不考虑外部节点是否为恶意节点的情况下利用动态非合作非零和博弈得到入侵检测分配策略，因此，在各阶段成功检测防御恶意节点的簇形结构数量较小。在第 6 个博弈阶段，本文方案成功检测防御恶意节点的数量迅速增加，基于贝叶斯规则的恶意节点后验概率不断更新较正，使博弈策略不断优化。第 13 个阶段开始，本文方案策略博弈达到一个稳定的状态。与文献[13]、文献[14]相比，本文方案在簇形结构的入侵检测方面有明显优势。

由于无线信号传输的不稳定性，WSNs 入侵检测方案需要具有较强的鲁棒性。在实验中不断改变参数 $a$ 和 $b$ 的取值，得到发送方 $S$ 和接收方 $R$ 在整个博弈过程中的收益函数变化情况如图 4 所示。其中，$|\Delta a|/a$ 表示 $a$ 的变化量与初值之间的比值，$|\Delta b|/b$ 表示 $b$ 的变化量与初值之间的比值，$|\Delta u_R|/u_R$ 为 $u_R$ 的变化量与初值之间的比值，初始时 $u_R$ 是在 $a = 0.9$ 和 $b = 0.06$ 条件下通过各入侵检测方案测得的。

文献[13]在簇形网络中构建恶意节点检测的状态空间和回归分析时未引入参数 $a$ 和 $b$，如图 4(a)和图 4(b)所示，当 $a$ 和 $b$ 变化量较大时，接收方 $R$

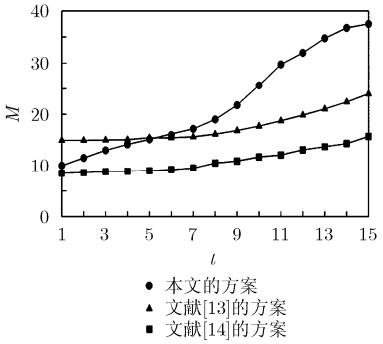
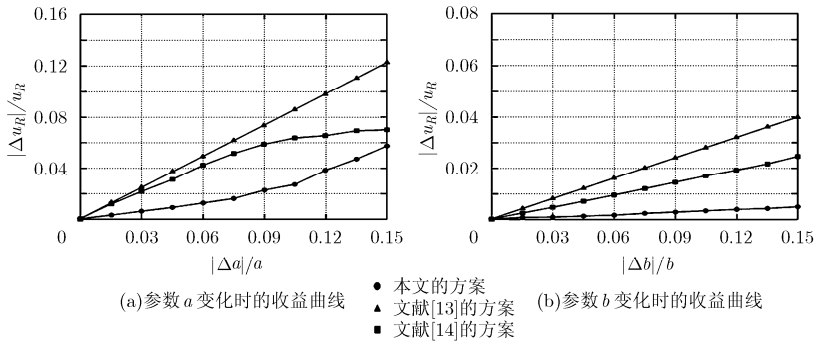



图3 不同阶段簇形结构检测成功数量对比




(a)参数 $a$ 变化时的收益曲线 (b)参数 $b$ 变化时的收益曲线

图4 不同方案的鲁棒性对比

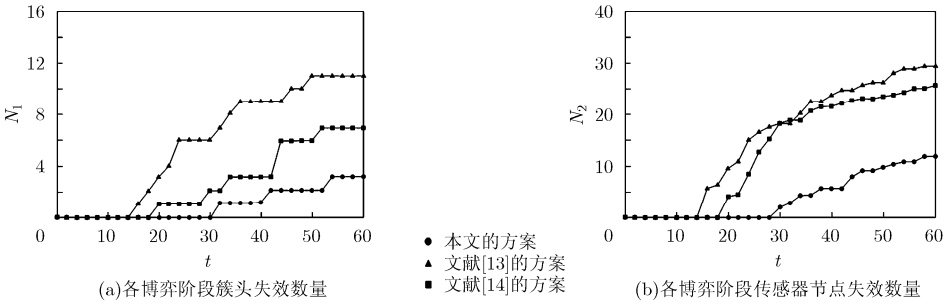
的收益值 $u_R$ 的波动幅度最大。而文献[14]中的Markov 动态博弈模型考虑了参数 $a$ 和 $b$ 对 $u_R$ 的影响，但没有将 $u_R$ 的取值与节点安全权值关联。因此，当改变 $a$ 和 $b$ 的值时，该方案 $u_R$ 的波动幅度均大于本文方案。图 4(a)和 4(b)中的实验结果表明，本文方案在 WSNs 多阶段入侵检测方面的鲁棒性明显优于文献[13]和文献[14]。

为验证本方案在资源有限的 WSNs 簇形结构中的性能，博弈阶段增加到 60 个，得到簇头和传感器节点的失效个数如图 5 所示。其中，$N_1$ 为 40 个簇形结构中累积失效簇头个数，$N_2$ 为累积失效传感器节点个数。

图 5(a)中给出了不同博弈阶段 $t$ 下执行各入侵检测方案的失效簇头个数对比。从 $t=15$ 开始，文献[13]的方案中簇头平均以每阶段 0.61%的速率失效，而文献[14]的方案平均每阶段失效的速率为 0.39%，这是由于基于马尔科夫模型的入侵检测“先听后说”机制提升了异常检测的性能，减缓了簇头节点的能量消耗。当每个博弈阶段 $Q$ 有限时，本文方案利用最少的节点资源达到最大的防御收益，放弃防御收益小于成本的传感器节点。在 60 个博弈阶段中，本文方案针对簇头能量消耗的鲁棒性最好。从图 5(b)中可以看出，本文方案在各阶段传感器节点失效数量最少。由于传感器节点与簇头通过合作关系共同防御入侵攻击，簇头在控制 $Q$ 消耗的同时，使节点的资源消耗得到优化。因此，本文方案更适于在资源有限的 WSNs 中应用。

## 6 结束语

本文在深入研究 WSNs 拓扑结构和信号博弈的基础上，建立了多阶段动态入侵检测博弈模型并给出了存在完美贝叶斯均衡的约束条件，提出了一种 WSNs 入侵检测最优策略方案。与其他入侵检测方案相比，本方案在利用贝叶斯规则更新外部节点为恶意节点的先验概率的同时给出了入侵检测系统的最优策略。仿真对比结果表明，本文模型和方案可有效检测和防御簇形 WSNs 中的恶意节点。




(a)各博弈阶段簇头失效数量 (b)各博弈阶段传感器节点失效数量

图 5 不同方案的失效节点对比

## 参 考 文 献

[1] 郁滨, 周伟伟. ZigBee 同频攻击检测抑制模型研究[J]. 电子与信息学报, 2015, 37(9): 2211–2217. doi: 10.11999/JEIT 141395.

YU B and ZHOU W W. Co-channel attack detection and suppression model for ZigBee network nodes[J]. *Journal of Electronics & Information Technology*, 2015, 37(9): 2211–2217. doi: 10.11999/JEIT141395.

[2] 杜晔, 张亚丹, 黎妹红, 等. 基于改进 FastICA 算法的入侵检测样本数据优化方法[J]. 通信学报, 2016, 37(1): 42–48. doi: 10.11959/j.issn.1000-436x.2016006.

DU Y, ZHANG Y D, LI M H, *et al*. Improved Fast ICA algorithm for data optimization processing in intrusion detection[J]. *Journal on Communications*, 2016, 37(1): 42–48. doi: 10.11959/j.issn.1000-436x.2016006.

[3] 杨安, 孙利民, 王小山, 等. 工业控制系统入侵检测技术综述[J]. 计算机研究与发展, 2016, 53(9): 2039–2054. doi: 10.7544/issn.1000-1239.2016.20150465.

YANG A, SUN L M, WANG X S, *et al*. Intrusion detection techniques for industrial control systems[J]. *Journal of Computer Research and Development*, 2016, 53(9): 2039–2054. doi: 10.7544/issn.1000-1239.2016.20150465.

[4] 赵婧, 魏彬, 罗鹏, 等. 基于隐马尔可夫模型的入侵检测方法[J]. 四川大学学报, 2016, 16(1): 106–110. doi: 10.15961/j.jsuese.2016.01.016.

ZHAO J, WEI B, LUO P, *et al*. Intrusion detection method based on hidden Markov model[J]. *Journal of Sichuan University*, 2016, 16(1): 106–110. doi: 10.15961 /j.jsuese.2016.01.016.

[5] KOLIAS C, KOLIAS V, and KAMBOURAKIS G. TermID: A distributed swarm intelligence-based approach for wireless intrusion detection[J]. *International Journal of Information Security*, 2016, 21(6): 1–16. doi: 10.1007/s10207-016-0335-z.

[6] YU Q, LYU J, JIANG L, *et al*. Traffic anomaly detection algorithm for wireless sensor networks based on improved exploitation of the GM (1, 1) model[J]. *International Journal of Distributed Sensor Networks*, 2016, 12(7): 218–227. doi: 10.1177/155014772181256.

[7] PATEL A, ALHUSSIAN H, PEDERSEN J M, *et al*. A nifty collaborative intrusion detection and prevention architecture for Smart Grid ecosystems[J]. *Computers & Security*, 2017, 64(2): 92–109. doi: 10.1016/j.cose.2016.07.002.

[8] KALNOOR G, AGARKHED J, and PATIL S R. Agent-based QoS routing for intrusion detection of sinkhole attack in clustered wireless sensor networks[C]. The First International Conference on Computational Intelligence and Informatics, Hyderabad, India, 2017: 571–583. doi: 10.1007/978-981-10-2471-9_55.

[9] WANG X Y, YANG L Z, and CHEN K F. Sleach: secure low-energy adaptive clustering hierarchy protocol for wireless sensor networks[J]. *Wuhan University Journal of Natural Sciences*, 2005, 10(1): 127–131. doi: 10.1007/BF02828633.

[10] FOROOTANINIA A and GHAZNAVI M B. An improved watchdog technique based on power-aware hierarchical design for ids in wireless sensor networks[J]. *International Journal of Network Security*, 2012, 4(4): 161–178. doi: 10.5121/ijnsa.2012.4411.

[11] DOUMIT S S and AGRAWAL D P. Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks[C]. Military Communications Conference, Alexandria, USA, 2003: 609–614. doi: 10.1109/MILCOM.2003.1290173.

[12] XIAO Z H, CHEN Z G, and DENG X H. Anomaly detection based on a multi-class CUSUM algorithm for WSN[J]. *Journal of Computers*, 2010, 5(2): 306–313. doi: 10.4304/jcp.5.2.306-313.

[13] JOKAR P and LEUNG V. Intrusion detection and prevention for ZigBee-based home area networks in smart grids[J]. *IEEE Transaction on Smart Grid*, 2016, 15(3): 1–12. doi: 10.1109/TSG.2016.2600585.

[14] MOOSAVI H and BUI F M. A game-theoretic framework for robust optimal intrusion detection in wireless sensor networks[J]. *IEEE Transactions on Information Forensics and Security*, 2014, 9(9): 1367–1379. doi: 10.1109/TIFS.2014.2332816.

周伟伟：　男，1990 年生，博士生，研究方向为无线传感器网络、物联网、信息安全技术.

郁　滨：　男，1964 年生，博士，教授，博士生导师，研究方向为无线传感器网络、视觉密码、信息安全技术.