无线传感器网络入侵检测的重复博弈建模研究

周四清[1,2],李志艳[2],刘 田[2]
ZHOU Si-qing[1,2],LI Zhi-yan[2],LIU Tian[2]

1.暨南大学 经济学院,广州 510632
2.暨南大学 信息科学技术学院,广州 510632
1.College of Economics,Jinan University,Guangzhou 510632,China
2.College of Information Science & Technology,Jinan University,Guangzhou 510632,China

ZHOU Si-qing,LI Zhi-yan,LIU Tian.Repeated game modeling for intrusion detection in wireless sensor network.Computer Engineering and Applications,2009,45(3):119-123.

Abstract: The lack of cooperation among the nodes of a network may seriously affect the network functions.In order to solve the problem,a repeated game framework,which optimizes packet forwarding probabilities of distributed nodes by detecting and responding the selfish behavior,is proposed.By the repeated game among nodes and broadcasting the monitored nodes' utility change,the framework could detect the selfish behavior in the network in time.A punishing mechanism which prevents the selfish nodes' deviation from cooperation is provided.The simulation results show that with the punishment mechanism in the model, selfish nodes can be forced to participate to the network operation and maintain the connectivity of network.
Key words: Wireless Sensor Network(WSN);intrusion detection;game theory;selfish node;repeated game

摘 要: 通过分析无线传感器网络节点影响网络可用性及其整体性能的自私行为,提出了一种无线传感器网络入侵检测的重复博弈模型,集中于检测和响应传感器节点的自私行为以加强网络节点的协作性能,利用节点与其邻居节点进行的重复博弈过程,广播节点的效用变化,即时检测出网络节点的自私行为。通过对网络节点的自私行为引入惩戒机制,从而大大降低了节点背离协作的可能性。仿真结果表明,对节点的自私行为实施惩戒机制,可以大大增强节点间相互协作,从而保证网络的连通性。
关键词: 无线传感器网络;入侵检测;博弈论;自私节点;重复博弈
DOI: 10.3778/j.issn.1002-8331.2009.03.035 **文章编号:** 1002-8331(2009)03-0119-05 **文献标识码:** A **中图分类号:** TP393

1 引言

无线传感器网络(Wireless Sensor Network,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[1-2]。

无线传感器网络是由大量的节点组成,缺乏固定的基础设施和集中控制机制[3]。在这种环境下,由于每个节点无线通信范围有限,需要相互协作将数据包传送到目的地。网络协作消耗能量,而无线传感器节点能量有限,因此并不是所有的节点都愿意参与协作。节点间缺乏协作是无线传感器网络出现的新问题,本文将其称为节点的"自私"行为,具有自私行为的节点称为自私节点。

自私节点在使用网络资源同时,拒绝耗费自身有限的能量为他人提供转发服务,即不协作参与网络的基本运行。由自私行为引起的损害不能被轻视。文献[4]仿真研究表明:当执行DSR 路由协议时,自私行为对整个网络中吞吐量和全网通信延时的影响,即使是很小一部分的自私节点也会使整个网络的吞吐性能严重降低。因此,如何检测及预防网络中节点的自私行为,从而保障传感器网络的可用性及其整体性能,逐渐成为其系统设计上需要考虑的一个关键问题。

文献[5]提出了一种基于 IDS(入侵检测系统)和自私节点间的重复博弈模型来检测和预防传感器网络中节点的自私行为,通过监测机制和声誉机制激励节点的协作行为。在传感器网络中,位于基站的 IDS 监视网络中其他节点的行为,并收集执行该功能后的观测结果,基于此建立起关于节点的声誉。IDS 利用该声誉值来评估节点的可信赖性并将结果发布给网络中的节点,并通过使用一个贴现因子从而与过去观测到的结果相关,泄漏一个经常发生变化的节点行为。信誉机制允许节点逐渐地隔离自私节点,因此,可以产生一组可信赖的传感器节点。但是,自私节点可以重新进入网络,他们参与网络协作从而使自身声誉上升。文献[5]证明了 IDS 和网络中节点都不从协作中背离的策略选择达到了纳什均衡。但是其均衡证明中,只考虑了 IDS 单方面背离的行为,并认为节点表现自私的原因是 IDS 的背离,而忽略了节点自私的天性,与实际不符。

因此,本文建立节点间的重复博弈模型对网络中存在的自私节点现象进行建模分析。

基金项目: 国家社科基金资助项目(No.06BJL066);暨南大学引进优秀人才科研启动基金资助项目(No.51205068)。
作者简介: 周四清(1964-),男,博士(后),副教授,主研方向:智能信息处理,能源金融;李志艳,硕士研究生;刘田,硕士研究生。
收稿日期: 2008-06-10 **修回日期:** 2008-08-27

2 无线传感器网络入侵检测的重复博弈模型

假设节点在每一时隙有两种策略行为选择:协作(即转发数据包),或者自私(即为保存电池能量丢弃接收到的数据包)。为分析方便,假设整个网络运行时间由一系列离散的协作时隙 t 构成,所有传送的数据包长度相同,且单一时隙长度足以保证每个数据包均能抵达目的节点。在任一时隙里,每个网络节点均有数据包需要发送,通过中继节点转发将数据包传送到目的地,并且在该时隙内由源节点和中继节点所构成的数据传输路由不发生改变,如果有一个中继节点拒绝转发,那么数据传输就失败了。

2.1 阶段博弈

假设网络中存在 N 个节点($N=\{1,\cdots,n\}$),源节点和目的节点集合为$\{S_i,D_i\}$,其中 $i=1,2,\cdots,M$。定义路由 $R_i=(S_i,f_{R_i}^1,f_{R_i}^2,\cdots,f_{R_i}^n,D_i)$,其中 S_i 和 D_i 分别表示源节点和目的节点,$I=\{f_{R_i}^1,f_{R_i}^2,\cdots,f_{R_i}^n\}$表示中继节点集合,即源节点发送的数据包经过 $n+1$ 跳到达目的节点。为简化分析,假定网络中所有的传输路由是预先确定的。设 $V=\{R_i:i=1,\cdots,M\}$为所有源目的对对应的路由集合。当节点 k 为源节点时,定义 $V_k^s=\{R_i:S(R_i)=k,i=1,\cdots,M\}$,其中 $S(R_i)$表示路由 R_i 的源节点。令节点 k 成功发送一个数据包的收益为 G(该收益包括了发送一个数据包的损耗),每转发一个数据包的损耗为 F,转发数据包的概率为 α_k(假定网络中所有节点的包转发概率相等),发送数据包到路由 i 的概率为 P_k^i,则 $\sum_{i=1}^{V_k^s}P_k^i=1$。因此,节点 k 的效用函数 U_k 可以表述为:

$$U_k=\sum_{i=1}^{V_k^s}\left(P_k^i\cdot G\cdot\prod_{j\in I_k^i}\alpha_j\right)-F\cdot\alpha_k\cdot B_k \tag{1}$$

其中 I_k^i 表示路由 i 上除源节点和目的节点以外的中继节点集合。B_k 是节点 k 接收到数据包的概率。

假设以节点 k 为中继节点的路由集合为 W_k,则 B_k 可表述为:

$$B_k=\sum_{r\in W_k}\left(P_{s(r)}^r\cdot\prod_{i\in\{f_r^1,f_r^2,\cdots,f_r^{m-1}\}}\alpha_i\right) \tag{2}$$

其中 $r=\{S(r),f_r^1,\cdots,f_r^{m-1},f_r^m=k,\cdots,f_r^n,D(r)\}$表示从源节点 $S(r)$ 到目的节点 $D(r)$的 $n+1$ 跳路由,第 m 个中继节点为节点 k,B_k 与路由 r 中节点 k 之前的所有节点的包转发概率有关。

假设节点是理性的,因此系统中所有节点都会调整自己的包转发概率实现自身效用最大化:

$$\max_{0\leqslant\alpha_k\leqslant 1}U_k(\alpha_k,\alpha_{-k}) \tag{3}$$

其中 $\alpha_{-k}=(\alpha_1,\cdots,\alpha_{k-1},\alpha_{k+1},\cdots,\alpha_N)$表示除节点 k 以外其他所有节点转发包的概率。

根据纳什均衡定义[6],当 $\alpha_k^*=0,\forall k$ 时,博弈将处于纳什均衡。即在任何场景下,所有节点都"永不合作"总是一种纳什均衡。从式(1)可以看出,所有节点的收益取决于其他节点转发数据包的概率,而与自己的行为无关,而节点的消耗仅取决于自己转发数据包的概率。因此每个节点有充分的理由丢弃接收到的数据包,从而减少能量损耗,增加自身效用,这相当于将 α_k 设置为尽可能小。但是,如果所有的节点都执行相同的策略,不转发数据包,则数据包成功传送的概率为 0,网络中将不存在任何协作行为,从而造成整个网络瘫痪。所以当所有节点处于纳什均衡状态,互不协作时,所有节点的收益均为 0,即 $U_k(\alpha_1^*,\cdots,\alpha_N^*)=0,\forall k$。此时,网络中的所有节点均为自私节点。

2.2 重复博弈

基于网络系统的动态特性,以及节点当前的行为选择会影响后继博弈阶段,相邻节点之间的交互已不再是一系列相互独立的单阶段博弈,而应当被整体地视为一个重复的多阶段扩展博弈过程,即构成一个重复博弈。假设该重复博弈具有已知的时间跨度 T,在每一时隙 t,节点可以观察到时隙 $1,\cdots,t-1$ 所有节点的行为,根据博弈论中以贴现因子 $\delta\in(0,1)$描述效用函数的形式[7],每个节点的总效用表述为:

$$\sum_{t=0}^{T}\delta^t U_k(\boldsymbol{\alpha}(t)) \tag{4}$$

其中,$\boldsymbol{\alpha}(t)=(\alpha_1,\cdots,\alpha_N)$。$U_k(\boldsymbol{\alpha}(t))$表示节点 k 在时隙 t 进行的阶段博弈的效用值。δ 可被视为对节点 k 协作耐心的综合度量:δ 越大,则表示 k 越耐心,也越重视长期利益;反之,则 k 越重视眼前利益。δ 的取值一般由网络性质与应用场景决定,临时构建的网络其值通常要小于长期存在的网络,而应用模式相对稳定的网络,δ 则要大于高度动态的网络。尽管节点携带的电池有限,即其生命周期有限,但是可以将节点间的博弈过程视为无限重复的,因为博弈双方都无法预知博弈何时终止。从博弈论的角度出发,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。这一假设在无线传感器网络的应用中是合理的。设 $T=\infty$,该博弈可视为无限重复博弈,则节点 k 的平均效用可表述为:

$$\overline{U}_k=(1-\delta)\sum_{t=0}^{\infty}\delta^t U_k(\boldsymbol{\alpha}(t)) \tag{5}$$

标准化因子$(1-\delta)$用来以统一的单位测度阶段博弈和重复博弈的收益:每期单元效用都标准化为 1。

重复博弈之所以能迫使自私节点进行合作,是因为如果节点在某一时隙表现自私,在之后的时隙里,其他节点将对该节点进行惩戒,从而使自私行为获得的收益在未来由于惩戒的损耗而被消除,因此所有节点都将表现为协作。下面引进一个惩戒机制来加强节点间的协作。

2.3 惩戒机制

为了对自私节点形成威慑,引入文献[8]中的惩戒机制,其基本思想是:如果在某一时隙,有节点表现自私(包转发概率下降),则从下一个时隙开始,网络中的其他节点集体孤立该自私节点,拒绝转发所有以该节点为源或目标的节点。假设惩戒时间为 T,通过这个惩戒机制,自私节点在背离时隙获得的短期收益将被 T 时间的惩戒消除。如果每个节点留意到通过理性参与者之假设,能够得到如式(5)所示的长期收益,那么所有的节点将没有动机从协作中背离。当一次博弈的纳什均衡为 $\boldsymbol{\alpha}^*=(\alpha_1^*,\cdots,\alpha_N^*)$,其效用函数为$(v_1^*,\cdots,v_N^*)=(U_1(\boldsymbol{\alpha}^*),\cdots,U_N(\boldsymbol{\alpha}^*))$。

设 $U=\{(v_1,\cdots,v_N)\mid\exists\boldsymbol{\alpha}\in\Omega^N\ (v_1,\cdots,v_N)=(U_1(\boldsymbol{\alpha}),\cdots,U_N(\boldsymbol{\alpha}))\}$,$V=$凸壳$\{U\}$,$V^+=\{(v_1,\cdots,v_N)\in V\mid v_k>v_k^*,\forall k\}$,其中 V 为可行收益集,V^+为帕累托占优于最小最大收益的可行收益集,这个集合是严格个人理性的。

令 $\boldsymbol{\alpha}=(\alpha_1,\cdots,\alpha_N)$为$(U_1(\boldsymbol{\alpha}),\cdots,U_N(\boldsymbol{\alpha}))$的联合策略。对于任一 $\varepsilon>0$,$(U_1(\boldsymbol{\alpha}),\cdots,U_{k-1}(\boldsymbol{\alpha}),U_k(\boldsymbol{\alpha})-\varepsilon,U_{k+1}(\boldsymbol{\alpha}),\cdots,U_N(\boldsymbol{\alpha}))\in V^+$。令节点 k 的最大效用为$\bar{v}_k=\max_{\boldsymbol{\alpha}}U_k(\boldsymbol{\alpha})$,$\forall k$,当其他节点都最大化节点 k 的效用时,取得该值。令协作效用为 $v_k=U_k(\boldsymbol{\alpha})\in V^+$,$\forall k$,当所有的节点执行协作的包转发概率时,取得该值。令节点被惩戒时,取得的效用最大值为 $\underline{v}_k=\max_{\alpha_k}[\min_{\alpha_{\neq k}}U_k(\boldsymbol{\alpha})]$。这个最大值 $\underline{v}_k$ 与一次博弈纳什均衡相对应。令节点被惩戒后,重新回到协作状态时,效用为 $v'_k=[U_k(\boldsymbol{\alpha})-\varepsilon]\in V^+$,$\forall k$。假设存在 ε,且节点 k 的惩戒时间为 T_k,使得:

$$\bar{v}_k/v'_k<(1+T_k) \tag{6}$$

设定如下步骤:

步骤 1　如果在前一博弈阶段,没有检测出自私节点,则所有的节点保持协作状态。如果检测出自私节点,则转向步骤 2(假设节点 k 背离)。

步骤 2　执行惩戒机制惩戒背离节点 k,在惩戒时期,网络中其他节点保持协作。

步骤 3　执行策略使得背离节点 k 的效用值为$(U_1,\cdots,U_{k-1},U_k-\varepsilon,U_{k+1},\cdots,U_N)$。如果在步骤 3 中存在背离行为,重新回到步骤 2,惩戒背离节点。

如果节点 k 背离后重新回到协作状态,则在背离时隙,它的收益最大,为$\bar{v}_k$,在惩戒时间 T_k 中,它的收益为 $\underline{v}_k$,当它再次回到协作状态,收益为 v'_k。因此节点 k 的平均折现效用值可以表述为:

$$\hat{U}_k=(1-\delta)\bar{v}_k+\delta(1-\delta^{T_k})\underline{v}_k+\delta^{T_k+1}v'_k \tag{7}$$

如果节点 k 在博弈过程中一直保持协作状态,它的平均折现效用值为:

$$U_k=(1-\delta)\sum_{t=0}^{\infty}\delta^t v_k=v_k \tag{8}$$

则节点 k 的背离收益可表述为:

$$\begin{aligned}\Delta U_k=\hat{U}_k-U_k&=(1-\delta)\bar{v}_k+\delta(1-\delta^{T_k})\underline{v}_k+\delta^{T_k+1}v'_k-v_k=\\&(1-\delta)\bar{v}_k+\delta(1-\delta^{T_k})\underline{v}_k+\delta^{T_k+1}(U_k-\varepsilon)-U_k<\\&(1-\delta)\bar{v}_k+\delta(1-\delta^{T_k})\underline{v}_k-(1-\delta^{T_k+1})(U_k-\varepsilon)\end{aligned} \tag{9}$$

令 $\underline{v}_k=0$,$\forall k$,当 $\delta\to1$ 时,$\dfrac{1-\delta^{T_k+1}}{1-\delta}\to1+T_k$。结合式(6),可以发现,式(9)中的背离收益将严格小于 0。这就意味着平均协作收益严格大于背离收益。因此,任何理性的节点将不会从协作状态中背离。

2.4　算法流程设计

为简化起见,在下面的描述中,省略了节点的下标。在初始化阶段,设置计时器 $n=0$,惩戒时间 $T=0$,包转发概率 $\alpha=\alpha_{\min}$,触发阈值 $V=U(\alpha)$。

如果所有节点相互协作,则每一个节点都将获得一个收益。但是,从式(1)可知:如果某节点在某一时隙从协作中背离即表现为拒绝转发数据包,而其他节点仍然保持协作,这个节点将会获得更多的收益,并且因为自己的自私行为使其他节点的收益降低。因此在每一时隙末,将每个节点的效用 U 与阈值 V 进行比较,如果 $U>V$,也就意味着,该节点从协作中背离,置计时器为 $n+1$,对自私节点执行惩戒,惩戒时间 $T=T+1$。在惩戒时间内,所有的节点集体孤立该自私节点,拒绝转发所有以该节点为源或目标的节点。假设所有的节点都是理性的,单次背离的收益迟早会被消除。因此,最后没有节点希望从协作中背离。预先设定一个常数 N,如果系统在时隙 N 达到稳定的协作状态,就假设协作被加强了,然后开始进入下一个阶段来改善目前的协作。

在下一阶段,该方案试图通过调整 α 使得节点达到最佳转发概率从而改善网络性能。在时隙末改变 α,然后在下一个时隙,所有的节点观察自己的性能是否有改善。如果没有,就把 α 的值恢复为原来的值,否则的话,节点设置 α 为其转发数据包的概率,并把阈值更新为当前的效用 $V=U$。

算法的具体流程如图 1 所示。

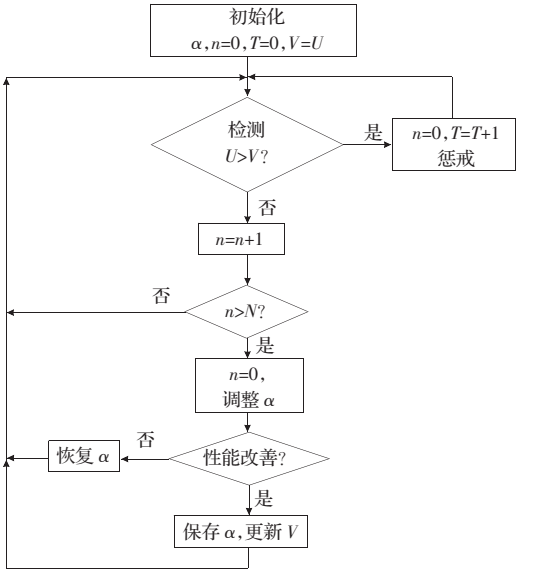

图 1　重复博弈流程图

在重复博弈阶段,由于惩戒机制的存在,只要贴现因子 δ 足够接近于 1,瞬间背离的收益迟早会被消除。在调整阶段,如果新的 α 值对于节点来说没有改善,α 将会恢复为原值。如果新的 α 值足够好,将会大大加强下一个阶段的重复博弈中节点的协作性。调整 α 的详细过程如下:给定 $\xi>0$,$\eta>0$。计算:

$$U_k^{t-1}(\alpha_k^{t-1}),U_k^{t-1}(\alpha_k^{t-1}+\xi),\Delta U_k^{t-1}=U_k^{t-1}(\alpha_k^{t-1}+\xi)-U_k^{t-1}(\alpha_k^{t-1})$$

如果:

$$\Delta U_k^{t-1}>0,\alpha_k^t=\alpha_k^{t-1}+\eta\frac{\Delta U_k^{t-1}}{U_k^{t-1}(\alpha_k^{t-1})},\alpha_k^t=\max(\min(\alpha_k^t,1),\alpha_{\min})$$

总的来说,该模型能检测出自私节点,并利用惩戒机制的

威胁在当前 α 的条件下维持协作，并能寻找到更利于协作的 α 值。

2.5 带延时的惩戒机制

在上一节中，假定节点知道整个网络的博弈行为，即无论节点在哪一时隙背离，所有节点都能即时检测出该自私节点。但是在实际的无线传感器网络中，由于庞大的开销，这样是不现实的。因此在本节中，假设每个节点只能观察到自己的博弈行为。因为节点不知道网络中其他部分的状况，而只知道自己所依赖的传输路由上是否有节点背离，所以不能检测出网络其他部分的背离行为。在网络中，只要有一个节点检测到背离行为，它就进入惩戒背离节点时期。这样，很有可能会触发另一个节点对该节点的惩戒行为。因为节点不能区分其他节点的策略改变是因为节点自身的背离，还是因为启动了对自私节点的惩戒。这个结果将会导致整个网络协作混乱。造成上述结果的原因是节点间对网络状态认知的不一致。它们不知道系统当前是处于惩戒阶段，背离阶段还是惩戒结束阶段、因此，在触发惩戒阶段中的任何错误都会导致所有网络节点的背离。

本文采用节点间泛洪广播来改善对网络状态一致认知的缺失问题。假设每个节点只观察其他一小部分节点的行为，在每一阶段博弈末期，节点广播是否有节点背离以及背离节点的位置。从而检测出自私节点并对其进行惩戒。

因此在上一节中的惩戒时期部分添加一个额外的步骤，即对自私节点进行惩戒前，节点将等待时间 T'，以保证网络中所有节点都接收到关于当前博弈结果的广播。这个时间 T' 被存储以保证网络状态的一致性。T' 的值取决于网络的规模和拓扑。如果 T' 的值太小，网络将不够稳定，而使惩戒时期占网络周期的大部分，因为某一用户延迟返回合作状态将会触发其他节点对它新一轮的惩戒。如果 T' 的值太大，它给自私节点以背离的机会，从而在不被其他节点察觉的情况下获取收益。因此在 T' 的数值选择上必须有所权衡。改进后的重复博弈流程图如图 2 所示。

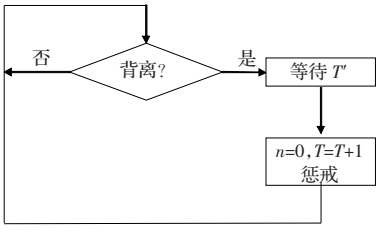

图 2 改进后的重复博弈阶段流程图

在网络达到稳定状态即 $n>N$ 后 α 的调整时期，可以通过泛洪广播让所有的节点同时改变他们的包转发概率。包转发概率改变之后，会对整个网络造成影响。所有的节点等待一个时间直到网络稳定。在这个时期末，节点得到他们新的效用值。如果这个效用值比原来的效用值好，就存储新的包转发概率。否则的话，就保留原来的包转发概率。该等待时间接近于 T'。

3 仿真与性能评估

仿真实验采用 MATLAB 7.0。为了评估提出的方案的性能，本文生成一个由 36 个节点组成的随机网络。网络中的节点随机分布在 100 m×100 m 的区域内，如图 3 所示。

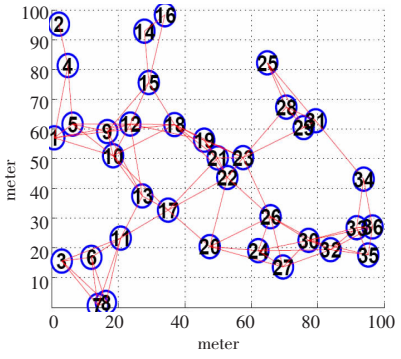

图 3 36 个节点组成的随机网络

假设发送的数据包能否到达目的地只取决于中继节点的包转发概率，如果某一节点表现自私，其策略选择为全部不转发接收到的数据包，而不包括选择性转发或随机转发。随机选择源节点和非邻居节点的目的节点，假定任意一个节点在一个时隙中均发送一个数据包。参数设定如下：贴现因子 δ=0.9，最小包传输概率 α_{min}=0，最大包转发概率 α_{max}=1，所有的算法初始化 $\alpha_k=\alpha_{min}, \forall k$。

图 4 显示了在不同的转发损耗比 F/G 下，包转发概率 α 对效用函数的影响。

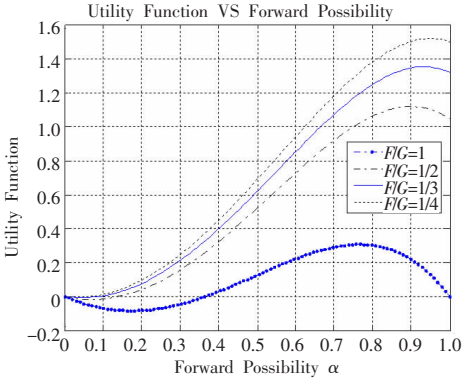

图 4 传送包概率对效用的影响

从图 4 可知，随着 F/G 的增大，节点的包转发概率下降，这就意味着所有节点消极参与转发数据包，从而使节点自身效用降低。这个现象是合理的，因为当转发损耗增加时，对于节点来说，为了自身数据包的传送，更好的策略是丢弃转接到的数据包，从而保存电池能量。因此合作机制的设计目标就是激励节点采取协作策略，从而达到一个全系统的最优转发概率。值得注意的是，节点不是采用所有大于 0 的数据包转发概率都会取得比在完全不协作状态下，即包转发概率为 0 时更大的效用。从图 4 可知，当 F/G=1 时，只有当 $\alpha\geqslant$0.37 的时候，节点的效用高于 0。因此在调整 α 阶段，如果 α 的取值小于 0.37，整个系统的性能表现将比非协作的时候还差。结果是新的 α 值被丢弃，恢复原来的 α 值。

图 5 显示了自私节点的平均效用。假设在重复博弈阶段，节点 7 在时隙 11 表现自私，从图中可以看出，由于节点背离协作，其背离时隙的效用值远远高于协作时的效用。通过相邻节点间的博弈，检测出该自私节点，则网络中所有节点通过广播更新其关于惩戒节点的记录，从时隙 12 开始对背离节点 7 进行惩戒，设置惩戒时间为 8。由于惩戒时间的存在，使得背离节

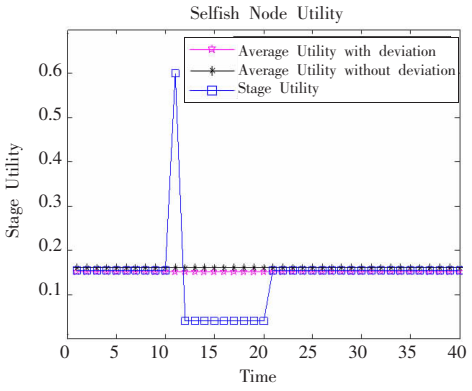

图 5　背离节点的平均效用

点的收益大大下降。很明显的,协作的平均收益将强于背离的平均收益。因此考虑到对自身将来收益的影响,任何节点均不会企图从协作中背离,因为这将降低其自身收益。

假设在时隙 N 网络达到稳定状态后,系统试图找到一个新的 α 值看能否改善系统性能。如果能,节点就采用新的 α,否则的话,就恢复为原有的 α 值。系统不断调整节点转发数据包的概率直到找到最优值。在这过程中,效用函数是一个不减少的函数。

假设 F/G=1,N=200,ξ=0.04,η=0.6,系统试图在 250 次实验中找到一个理想的 α。观察随着时间变化的效用和包转发概率,如图 6 所示。从图 6 可以看出,最大包转发概率接近于最优值,并能通过调整 ξ、η 的取值,使得网络节点在确定的时间内较快地取得最大包转发概率。

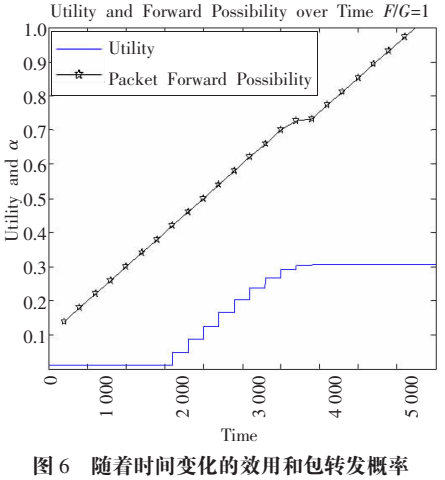

图 6　随着时间变化的效用和包转发概率

图 7 和图 8 分别显示了在理想情况和实验情况下,包转发概率以及节点效用同转发损耗比 F/G 的关系。从图中可以看出,仿真结果能以 0.13%和 1.56%的偏差范围逼近理想化的包转发概率和效用,从而证明了提出的方案能有效地找到最优包转发概率。

4　小结

在分析传感器网络中存在的节点自私行为的基础上,运用重复博弈理论,提出了针对自私节点攻击的入侵检测方案。该方案通过节点与其相邻节点间的重复博弈过程,检测出自私节点并对其进行惩戒,通过设置惩戒时间消除自私节点背离获得的收益。考虑到对未来收益的影响,理性节点将采取合作策略

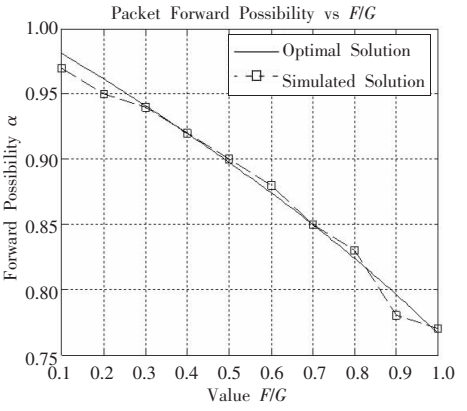

图 7　F/G 对最优包转发概率的影响

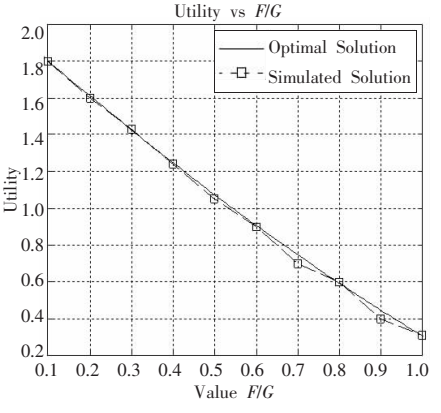

图 8　F/G 对最优效用的影响

从而保证了网络的连通性。从仿真结果可以看出,提出的方案可以使节点在当前包转发概率下保持协作状态。同时系统在稳定状态下调整 α,从而使节点在采用一个较高的包转发概率的同时效用增加,这样有效地遏制节点为保存自身能量,拒绝转发数据包的自私行为。当有计划地设定每个节点最优包转发概率时,通过未来惩戒机制的威胁,可以大大增强节点间的相互协作,从而保持了网络的连通性。

参考文献:

[1] Tilak S,Abu-Ghazaleh N B,Heinzelman W.A taxonomy of wireless micro-sensor network models[J].Mobile Computing and Communications Review,2002,1(2):1-8.

[2] 孙利民,李建中,陈渝,等.无线传感器网络[M].北京:清华大学出版社,2005.

[3] 于海斌,曾鹏,梁韡.智能无线传感器网络系统[M].北京:科学出版社,2006.

[4] Michiardi P,Molva R.Simulation-based analysis of security exposures in mobile Ad hoc networks[C]//European Wireless Conference,2002.

[5] Agah A,Das 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.

[6] 张维迎.博弈论与信息经济学[M].上海:上海人民出版社,1996.

[7] 朱·弗登博格,让·梯若尔.博弈论[M].北京:中国人民大学出版社,2002.

[8] Altman E,Kherani A A,Michiardiy P,et al.Non-cooperative forwarding in ad-hoc networks[C]//Proc of the IFIP Networking 2005.Heidelberg:Springer-Berlin,2005:486-498.