文章编号：2095-4980(2022)02-0181-07

基于博弈论的无线传感网络节点攻防优化

周全兴[1]，李秋贤*[1]，王振龙[1]，吴雨龙[2]

(1.凯里学院 大数据工程学院，贵州 凯里 556011；2.贵州大学 计算机科学与技术学院，贵州 贵阳 550025)

摘　要：针对无线传感器网络各节点在安全需求与资源消耗上存在的矛盾，提出一种基于博弈论的无线传感网络节点优化博弈模型。首先，通过分析网络节点中攻击方的攻击代价与防守方的防守开销，基于博弈论分析攻防双方的效用函数并构造攻防博弈模型；其次，根据网络节点中攻防双方选择的不同行动策略，结合信息论技术将攻防双方抽象成随机变量，并设计博弈信道模型；接着，由信道容量与纳什均衡融合定理分析攻击方的攻击代价与防守方的防守开销，当博弈双方的效用达到纳什均衡时与信道容量相等，此时双方采用的行动策略即为博弈的纳什均衡解；最后，对设计的模型进行实验与仿真，结果表明，该模型在保证无线传感网络安全性的前提下，有效地降低了网络系统的防守开销，延长了网络系统的生命周期。

关键词：博弈论；信息论；无线网络节点；攻防博弈模型；纳什均衡

中图分类号：TN915.08；TP393　　**文献标志码：**A　　**doi：**10.11805/TKYDA2020659

Attack and defense optimization of wireless sensor network nodes based on game theory

ZHOU Quanxing[1]，LI Qiuxian*[1]，WANG Zhenlong[1]，WU Yulong[2]

(1.College of Big Data Engineering，Kaili University，Kaili Guizhou 556011，China；
2.College of Computer Science and Technology，Guizhou University，Guiyang Guizhou 550025，China)

Abstract：Aiming at the contradiction between security requirements and resource consumption of wireless network nodes，a wireless sensor network node optimization game model is proposed based on game theory. Firstly，by analyzing the attack cost of the attacker and the defense cost of the defender in the network node，the utility function of the offense and defense is analyzed based on game theory，and the offense and defense game model is constructed. Secondly，according to the different action strategies selected by the offensive and defensive parties in the network node，combined with information theory technology，the offensive and defensive parties are abstracted into random variables，and the game channel model is designed. Then，the attack cost of the attacker and the defense cost of the defender are analyzed according to the channel capacity and Nash equilibrium fusion theorem. When the utility of both parties in the game reaches the Nash equilibrium，it is equal to the channel capacity. At this time，the action strategy adopted by both parties is the Nash equilibrium solution of the game. Finally，through experiments and simulations on the designed model，the results show that the model effectively reduces the defense overhead of the network system and prolongs the life cycle of the network system while ensuring the security of the wireless transmission network.

Keywords：game theory；information theory；wireless network node；attack-defense game model；Nash equilibrium

无线传感器网络由于其具有适合大规模部署且低能耗等特点而被广泛应用于军事、医疗、农业和工业等领

收稿日期：2020-11-27；**修回日期：**2021-01-02

基金项目：凯里学院专项课题资助项目(YQZX201907)；国家自然科学基金资助项目(61772008；教育部—中国移动科研基金研发资助项目(MCM20170401；贵州省教育厅青年科技人才成长资助项目(QianjiaoheKY [2020]179,[2020]180)

*通信作者：李秋贤　email:547230161@qq.com

域[1−2]。大规模分布式传感器系统是一个专家系统，可以将原始传感器数据与空间信息结合起来执行复杂的信号处理任务，这种能力在军事应用中的监视或目标跟踪、气温湿度等事件监视、协作波束形成等应用场景中是必不可少的[3−4]。随着无线传感器网络技术的广泛应用，无线传感器网络的安全需求也变得越发急迫和重要。然而，无线传感器网络由于网络系统的资源限制和苛刻的部署环境，提供可靠、可扩展的安全网络通信比传统网络更具挑战性。无线传感器网络所带来的独特挑战包括有限的存储、计算资源和通信带宽，以及大量节点分布在没有预先存在的基础设施的区域内[5−6]，这使得人们在提高其安全性的同时还面临着有效管理能源从而延长网络寿命的挑战。基于无线传感器网络节点攻防消耗以及其安全性需求，传感器节点需要部署入侵检测、身份认证的安全技术手段来抵御恶意的攻击，持续地运行这些安全技术需要消耗大量的能量从而导致网络寿命大大缩短。面对无线传感器网络在安全性与资源消耗问题上的矛盾，许多研究工作基于博弈论进行展开[7−9]。博弈论是研究两个或多个参与者谋略和决策问题的理论[10−11]，每一个参与者要选择的策略必须是针对其他参与者选择战略的最优反应，每一个参与者都希望尽可能提高自己的利益所得。由于博弈论提供了描述自私和恶意节点所带来问题的方法，因此它可以作为分析无线传感器网络的有利工具，其中，优化各种节点活动的能量消耗和实现安全的网络操作可以建模为以节点为参与者的博弈[12−13]。国内外已有很多学者在博弈论框架下对无线传感器网络进行研究。Juan[14]提出了一种退避攻击下的无线传感网博弈模型，利用基于后悔匹配的算法来寻找博弈的均衡解。Ma[15]等人提出了一种无线传感网的入侵检测系统(Intrusion Detection Systems，IDS)博弈模型，该方法将 IDS 部署于簇头节点上，利用簇头节点来检测簇内普通节点的行为是否存在恶意攻击。Ahmed[16]等人利用进化博弈的思想提出了一种无线传感器网络的自私节点激励机制，以奖励的方式鼓励节点参与正常的通信而非选择恶意攻击。Yang[17]等人提出了一种基于动态行为监控博弈的无线传感器网络聚类信息评估方案，并将其集成到簇的路由协议当中。Liao[18]等人提出了一种基于混合连续策略监控的前向博弈选择转发方案来缓解选择转发攻击。Lakshman[19]等人采用了一种双方零和博弈模型来分析最大检测几率下的网络系统开销。Chen[20]等人提出了一种基于进化博弈模型的无线传感器网络主动防御模型，该模型强调节点从攻击者的不同攻击策略中学习理性进化的能力是有限的，并且能够动态调整其策略以实现最有效的防御。Qiu[21]等人提出了一种节点进化学习合理性有限的无线传感器网络主动防御模型来调整防御策略。Yang[22]提出一种基于博弈论的集群无线传感器网络能耗均衡方法来提高网络的输出周期。Lin 等[23]基于 Stackelberg 博弈模型，提出无线定位网络功率分配方案，降低了网络误差，并提高了网络定位的精确度。

整体上看，当前的方案主要存在以下问题：对于恶意节点的处罚是一个与防守方无关的参数。这代表着处罚的大小是不固定的。对于无线传感器网络的建立者而言，此时会尽可能地增大处罚从而降低恶意节点的效用，试图达到降低恶意节点发动攻击的可能性。但是在这种情况下，防守方可能会为了高额的处罚金而尽可能地提高自身执行检测和监督等行为的可能，从而造成了大量的资源损耗。仅将方案部署于簇头节点上，利用簇头节点来检测簇内普通节点的行为是否存在恶意攻击。这种方法在一定程度上降低了无线传感网当中的资源损耗，但是仅仅依靠簇头以某种概率执行检测并不足以满足无线传感器网络的安全需求，同时簇头节点执行的检测是面向簇内每一个节点的，因此簇头节点的能量损耗过大，严重影响了簇头节点的生命周期。

针对上述问题，本文在详细分析双方攻防效用的前提下，结合博弈理论提出一种基于博弈论的无线传感器网络节点攻防优化模型。

1 基础知识

本节介绍在建模及分析过程中运用到的博弈论和信息论及相关背景知识。

1.1 博弈论

博弈论表达的基本形式由三个要素组成，即局中人集合 P、策略空间 S 和效用函数 u，即 $G=\{P,S,u\}$，其中，$P=\{P_1,P_2,\cdots,P_n\}$，$S=\{S_1,S_2,\cdots,S_n\}$，$u=\{u_1,u_2,\cdots,u_n\}$。效用函数 $u_i:S\to R$，效用函数中 u_i 表示第 i 个理性参与者在选择不同的行动策略情况下获得的不同的收益。

1.2 纳什均衡

纳什均衡又称为非合作博弈均衡，即在 n 个参与者的标准式博弈 $G=\{S_1,S_2,\cdots,S_n;\ u_1,u_2,\cdots,u_n\}$ 中，如果 n 是有限的，且对于每个 i，S_i 也是有限的，则博弈至少存在一个纳什均衡，均衡可能包含混合策略。

具体的纳什均衡是指所有参与者存在一种策略组合，在该策略组合中，任何一个参与者改变其行动策略都

不会得到好处，即在任何博弈中，无论是纯战略还是混合战略的纳什均衡都表现为参与者的一个最优反应对应的一个交点。

1.3 互信息量

信源发出消息 x 的概率 $p(x)$ 为先验概率；信宿收到消息 y 之后推测信源发出 x 的概率 $p(x,y)$。互信息量是指由另一个随机变量导致的，原随机变量不确定度的缩减量，这个缩减量就是互信息量，也可以视作一个随机变量由于另一个随机变量而减少的不确定性。其形式化定义为：$I(X,Y)=\sum_{x\in X}\sum_{y\in Y}p(x,y)\log\frac{p(x,y)}{p(x)p(y)}$。

1.4 信道容量与纳什均衡融合定理

信道容量与纳什均衡融合定理[24]是指：当信道固定时，若以输入和输出之间的互信息作为收益函数，那么两方之间的标准式博弈一定存在纯策略的纳什均衡解，而且当达到纳什均衡时，它们的收益函数刚好就是信道容量。

2　无线传感器网络节点博弈模型

2.1 系统模型

分层的簇状网络模型已被证明能够有效降低能耗，延长网络生命周期[25]。因此本文采用分层的网络模型，将无线传感器网络中的传感器节点进行分簇[26]。每个簇都包含一个簇头节点和多个普通节点。普通节点的工作主要是收集数据，并向簇头节点发送数据包。簇头节点的任务则是收集簇内的信息进行融合并发送给基站，如图 1 所示。

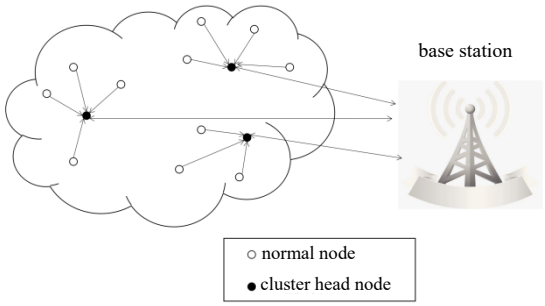


Fig.1 Clustering network model
图 1 分簇网络模型

在本文提出的博弈模型中，每一个节点都是理性和自私且各自为政的，每个节点都能够在恶意节点存在的恶意环境下争取更多收益，这表示各节点总是期望提高自身的收益，同时也会根据自身的目的来考虑是否对进行通信的节点进行入侵检测或监督。越频繁地执行检测和监督将会造成越大的能耗，恶意节点总是期望发动攻击以取得更多的效用，而当恶意节点的恶意行为被捕获到时，为避免无限制地设置处罚而造成节点因持续执行检测和监督造成更多的能耗，恶意节点以支付节点的检测或监督能耗作为处罚。

2.2 形式化定义

本文设计的无线传感器网络博弈模型是一个三元组 (N,S,U)。其中，N 代表博弈中的所有参与者的集合；S 代表博弈中各参与者可能采取的行动策略集合；U 代表博弈中各参与方的效用函数集合。

2.3 参与者

参与者集合 N 由参与博弈的攻击节点 N_{Att} 和防守节点 N_{Def} 组成，即 $N=\{N_{\mathrm{Att}},N_{\mathrm{Def}}\}$。每个参与方都是理性的，这表示攻防双方在博弈过程中，总是以追求自身利益最大化为目的而采取行动的。

2.4 行动策略集合

行动策略集合是参与博弈的无线传感网络节点攻防双方所能采取的所有行动策略的集合，即可以表示为：$S=\{S_{\mathrm{Att}},S_{\mathrm{Def}}\}$。其中攻击无线传感网络节点的混合策略为：$S_{\mathrm{Att}}=\{p,1-p\}$，$p$ 代表攻击节点为获取更高收益而发动攻击概率，$1-p$ 代表为避免恶意行为被发现，而不发动攻击的概率。防守网络节点的混合策略为：$S_{\mathrm{Def}}=\{q,1-q\}$，$q$ 代表防守节点为抵抗攻击而执行检测和监督的概率，$1-q$ 代表为节省消耗而不执行检测和监督的概率。

2.5 效用函数

效用函数集合由博弈中的攻防双方在不同的策略组合下的效用组成，即 $U=\{U_{\mathrm{Att}},U_{\mathrm{Def}}\}$。其中，$U_{\mathrm{Att}}$ 代表攻击节点的效用，U_{Def} 代表防守节点的效用。本文的博弈模型中，考虑从信息论的角度设计双方的效用函数。

对于攻防双方而言，无论对方采取哪一个行动，自身的行动策略集合中总是存在一个对应的最优响应。例

如，对于防守方而言，如果得知对方将采取攻击，那么此时最优的行动策略则是执行入侵检测等防御手段。在信息论当中，互信息量代表一个随机变量因为了解到另一个随机变量而减少的不确定度。如果将攻防双方的行动抽象成随机变量，那么此时双方所争取的则是尽可能地提高自身对于对方的互信息量，从而可以更有利地做出行动策略的选择。对于当前的标准式博弈 $G=\{N_{\mathrm{Att}},N_{\mathrm{Def}};U_{\mathrm{Att}},U_{\mathrm{Def}}\}$ 而言，它有两个参与者，分别是防守方 X 和攻击方 Y。双方采取的行动有限，即防守方只能采取执行入侵检测等安全技术或者不执行；攻击方只能采取发动攻击或者不攻击。此时攻击方的收益函数和防御方的收益函数就可以定义为：$U_{\mathrm{Att}}=I(Y,X)$，$U_{\mathrm{Def}}=I(X,Y)$。

为了激励所有节点都正常地参与活动，需要对发动攻击而被捕获做出惩罚，而执行入侵检测等安全技术则会造成防守开销。同时为了避免防守节点为了高额罚金而持续地执行检测，对于恶意节点的处罚设置也是受限的。据此定义参数：E_C 代表防守节点执行检测所消耗的能量，E_A 代表攻击节点发动攻击所消耗的能量，E_M 代表攻击节点等待攻击所消耗的能量，U_i 代表节点正常通信所产生的收益。当攻击节点发动攻击被防守节点捕获时，其不仅消耗了发动攻击所需的能量代价，还需要对防守节点执行检测所产生的代价进行赔付，而防守节点成功地抵御了攻击，因此获得节点运转的收益；当攻击节点发动攻击且没有被捕获时，其成功地攻击了节点并取得该节点收益，而防守节点失去其正常运转的收益；当攻击节点不进行攻击时，攻击节点将花费能量来伪装正常的通信行为，等待并准备下一次攻击；若防守节点此时执行检测，那么防守节点将花费执行检测的代价；若防守节点不执行检测，则获得本次运转的全部收益。

在博弈过程中，攻击节点为了获得更高的效用总是想要发动攻击，然而过于频繁的攻击会增加自身攻击行为被发现和捕获的风险；防守节点为避免遭到攻击而承受损失，会执行检测行动来抵抗攻击，然而过于频繁地执行检测行动会造成大量检测开销。在本文设计的博弈模型中，攻击者被捕获时受到的处罚恰好等于防守方的检测损耗 E_C 而非单独设置一个惩罚代价，这是因为一个高额的罚金会导致攻击方减少攻击行为，与此同时防守方为追求高额罚金而尽可能地提升检测概率，从而造成更多不必要的检测开销。

3 博弈模型分析

在本方案中，对于无线传感网络节点的数据或网络环境的绝对安全性并未强制要求，其网络节点的效益取决于节点的自利行为。在本文假设中，对于防守方而言，如果被攻击，必然遭受损失。此时防守方进行防守，则承担计算损耗，不进行防守，则遭受数据失窃、网络可用性受损等价值损失。如果过度防守，会消耗过多计算资源而得不偿失，过少防守则会导致安全性风险带来价值损失。此时对于防守方而言，考虑的是防守开销和容忍入侵损失之间的权衡。然而对于攻击方而言，发动攻击，需要付出攻击代价。攻击成功，就会带来一定的效益。当防守方抵抗概率很高时，频繁攻击显然带来更高的攻击消耗。因此本文的博弈讨论，在于防守方的入侵容忍度和攻击方的攻击成本损失度的均衡。

对于攻击节点而言，它总是企图通过发动攻击来获取更高的收益，但是过于频繁地发动攻击则会大大提高暴露的风险。对于防守节点而言，它总是期望执行检测等安全手段来抵御攻击以降低遭受攻击的损失，但是过于频繁地执行检测等安全手段将会增大其防御开销，造成过度防御而得不偿失的情况。因此双方会不断地调整行动策略，以期望能在博弈中获得最大收益。如果对于攻击节点而言，若存在一个策略 S_{Att}^{*} 是其对于防守节点采用策略 S_{Def}^{*} 的最优响应，同时对于防守节点而言策略 S_{Def}^{*} 也是其对于攻击节点采用策略 S_{Att}^{*} 的最优响应，那么策略组合 $\left(S_{\mathrm{Att}}^{*},S_{\mathrm{Def}}^{*}\right)$ 就是博弈的纳什均衡解。此时，任何一方都不能通过调整自身收益而获得更高的效用，这代表：$\begin{cases}U_{\mathrm{Att}}\left(S_{\mathrm{Att}}^{*},S_{\mathrm{Def}}^{*}\right)\geqslant U_{\mathrm{Att}}\left(S_{\mathrm{Att}}^{*},S_{\mathrm{Def}}^{*}\right)\\U_{\mathrm{Def}}\left(S_{\mathrm{Att}}^{*},S_{\mathrm{Def}}^{*}\right)\geqslant U_{\mathrm{Def}}\left(S_{\mathrm{Att}}^{*},S_{\mathrm{Def}}^{*}\right)\end{cases}$。实现博弈攻防双方的执行步骤如下所示：

Step1：方案初始化，通过分析网络节点中攻击方的攻击代价与防守方的防守开销，利用博弈论设计无线传感网络节点的博弈模型，其模型包括参与者、行动策略集合和效用函数；

Step2：在博弈模型中，攻防双方节点根据其自利行为选择对应的行动策略，假设攻击方选择的策略为 S_{Att}^{*}，防守方选择的策略为 S_{Def}^{*}；

Step3：由攻防双方选择的行动策略，得到攻击方获得的效用 U_{Att}，防守方获得的效用 U_{Def}，直到双方获得最优响应；

Step4：根据信道容量与纳什均衡融合定理，当攻防双方获得最优响应时，分析博弈双方的效用函数与信道容量，若相等，此时双方采用的行动策略即为博弈的纳什均衡解；否则将继续返回第二步。

表 1 双方自评

Table1 Self-evaluation by both parties

action combination	X	Y	event probability
launch an attack, perform detection	1	0	pq
launch an attack, do not perform detection	0	1	$p(1-q)$
no attack, perform detection	0	0	$(1-p)\,q$
no attack, do not perform detection	1	0	$(1-p)\,(1-q)$

对于一个双方的标准式博弈而言，若以一方作为输入，另一方作为输出，那么该标准博弈一定存在纯战略的纳什均衡，而且当达到均衡时，它们的收益函数就刚好是双方构成信道的信道容量[24]。因此，将代表防守方随机变量 X，将代表攻击方随机变量 Y，定义为根据双方所采取的不同行动组合，双方以提高自身效用为目的，产生一个自评来评价本次博弈的成败，双方自评如表 1 所示。根据双方的行动策略组合，将会有以下几种情况：

1) 攻击方发动攻击，防守方执行入侵检测系统等相关安全技术。此时攻击方的攻击行为将会被防守方捕获从而受到惩罚，而防守方获得了罚金而弥补了防守开销。因此这种情况下攻击方自评为失败，防守方自评为成功。当前事件的概率及双方自评结果记为：P(攻击,检测)= pq，X=1,Y=0。

2) 攻击方发动攻击，防守方没有执行入侵检测系统等相关安全技术。此时攻击方成功地攻击了某簇节点而获得额外收益，防守方因遭受攻击而承受损失。这种情况下，攻击方自评为成功，防守方自评为失败。当前事件的概率及双方自评结果记为：P(攻击,未检测)= $p(1-q)$，X=0,Y=1。

3) 攻击方未发动攻击，防守方执行入侵检测系统等相关安全技术。此时攻击方因放弃攻击而承担等待攻击所带来的消耗，防守方因为过度防御而承担了防守开销。这种情况下，攻击方和防守方的自评都为失败。当前事件的概率及双方自评结果记为：P(未攻击,检测)= $(1-p)q$，X=0,Y=0。

4) 攻击方未发动攻击，防守方没有执行入侵检测系统等相关安全技术。此时攻击方因放弃攻击而承担等待攻击所带来的消耗，而防守方明智地没有执行过度防御减少其能量消耗。在这种情况下，攻击方的自评为失败，防守方自评为成功。当前事件的概率及双方自评结果记为：P(未攻击,未检测)= $(1-p)(1-q)$，X=1,Y=0。

有 $P(X=1)=pq+(1-p)(1-q)$, $P(X=0)=p(1-q)+(1-p)q$, $P(Y=1)=p(1-q)$, $P(Y=0)=pq+(1-p)q+(1-p)(1-q)$,

$$P(X=0,Y=0)=\frac{P(Y=0\mid X=0)}{P(X=0)}=\frac{(1-p)q}{p(1-q)+(1-p)q},\quad P(X=0,Y=1)=\frac{P(Y=1\mid X=0)}{P(X=0)}=\frac{p(1-q)}{p(1-q)+(1-p)q},$$

$$P(X=1,Y=0)=\frac{P(X=1\mid Y=0)}{P(Y=0)}=\frac{pq+(1-p)(1-q)}{pq+(1-p)q+(1-p)(1-q)},\quad P(X=1,Y=1)=\frac{P(X=1\mid Y=1)}{P(Y=1)}=0$$

此时，以随机变量 X 作为输入，以随机变量 Y 作为输出(以随机变量 Y 作为输入，以随机变量 X 作为输出是一样的)，建立起博弈信道。根据前文所述，双方会根据自身目的不断地调整行动概率策略 (p,q)。在本方案中，由设计的博弈模型可知参与博弈的网络节点攻防双方的行动策略集合为 $S=\{S_{\text{Att}},S_{\text{Def}}\}$，其中攻击方的行动策略为 S_{Att}，攻击无线传感网络节点的混合策略为：$S_{\text{Att}}=\{p,1-p\}$，p 代表攻击节点为获取更高收益而发动攻击概率，$1-p$ 代表为避免恶意行为被发现，而不发动攻击的概率。防守方的行动策略为 S_{Def}，防守网络节点的混合策略为：$S_{\text{Def}}=\{q,1-q\}$，q 代表防守节点为抵抗攻击而执行检测和监督的概率，$1-q$ 代表为节省消耗而不执行检测和监督的概率，由此可知攻防双方的行动策略集合 $S=\{S_{\text{Att}},S_{\text{Def}}\}$ 是依照概率组合 (p,q) 分布的。而博弈双方行动策略的变化，将导致输入信号 X 和输出信号 Y 的互信息量 $I(X,Y)$ 不断变化。直至某一时刻，当攻防双方采取了某一行动策略 (p^*,q^*) 时，互信息量 $I(X,Y)$ 达到最大值并且等于博弈信道的信道容量 D，此时博弈达到均衡。而 (p^*,q^*) 就是博弈的纳什均衡解。据此，只要得到了博弈信道的信道容量，那么博弈的纳什均衡解就可以确定了。博弈信道的信道容量可以计算为：

$$D=\max_{0\leqslant p,q\leqslant 1}[I(X,Y)]=\sum_x\sum_y P(x,y)\log\frac{P(x,y)}{P(x)P(y)}=P(X=0,Y=0)\log\frac{P(X=0,Y=0)}{P(X=0)P(Y=0)}+P(X=0,Y=1)\log\frac{P(X=0,Y=1)}{P(X=0)P(Y=1)}+$$
$$P(X=1,Y=0)\log\frac{P(X=1,Y=0)}{P(X=1)P(Y=0)}+P(X=1,Y=1)\log\frac{P(X=1,Y=1)}{P(X=1)P(Y=1)}$$

4　仿真实验

4.1 实验参数

仿真实验在 Glomosim 平台进行。在 100 m×100 m 的范围内随机部署 100 个节点，每个节点的能量初始化为 50 J，其中随机地存在 10 个恶意节点，相关设置如表 2 所示。

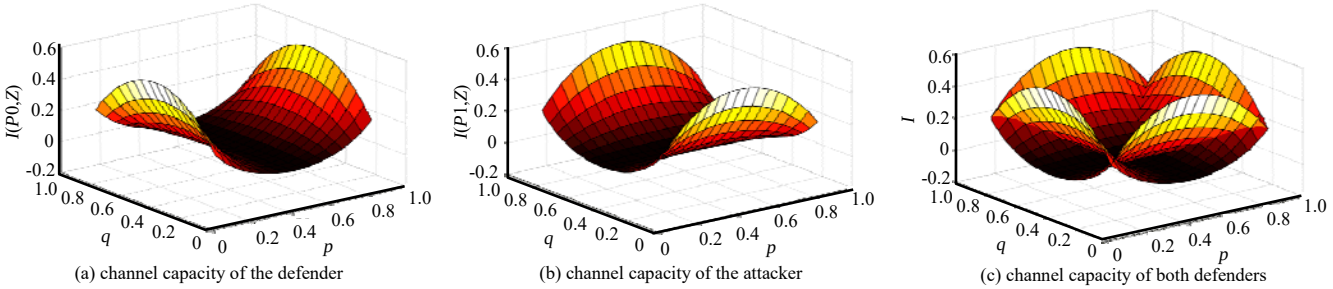
表 2 实验相关参数

Table2 Experimental parameters

parameter	simulation set
range/m	100×100
number of nodes	100
number of malicious nodes	10
node placement strategy	randomly placed
node initial energy/J	50
E_C/J	3
E_A/J	2
E_M/J	1
wireless receiving packet mode	error-free transmission
simulation time/min	15

4.2 实验结果及分析

根据第 3 节得到的博弈信道的信道容量取值如图 2 所示，根据随机变量 X 与 Y 的变化，分别从不同维度做实验仿真，如图 2 所示。每个节点每分钟会更新一次行动策略，行动策略的调整将依据上一分钟的检测次数或被捕获次数的统计量以及对应在表 1 中的取值进行调整，双方行动策略的初始值($p=0.5$ ， $q=0.5$)。



(a) channel capacity of the defender (b) channel capacity of the attacker (c) channel capacity of both defenders

Fig.2 Channel capacity in the game channel

图 2 博弈信道中的信道容量

由于传感器节点的资源是有限的，因此其能量消耗是维持网络生命周期的关键因素。无线传感网中，大部分能量消耗在无线通信上[27]，除此之外传感器节点执行检测的行为也极大地增加了自身开销。对于全监督方案(即每个节点持续执行检测)而言，由于其持续地运行检测等防御手段，传感器节点消耗了大量的能量，因此其节点失效速度最快，网络生命周期也最短。在 Juan[14]等人的方案中，由于只分析和考虑整个网络中只存在一个恶意节点的情况，因此在恶意节点不唯一时，并不能有效地降低网络系统中的总体消耗。从图 3 中可以看出，基于本文博弈模型的检测方案的节点平均能量消耗相较于全监督方案和 Juan[14]等人的方案相对缓慢，无线传感网的网络生命周期将相对更长，因此本文提出的基于信息论的无线传感网博弈均衡方案有效地解决了无线传感网当中资源受限和检测开销的问题。为对比方案的准确检测率，定义以下指标：准确率=$\frac{\text{检测到的攻击}}{\text{所有攻击数量}}$。

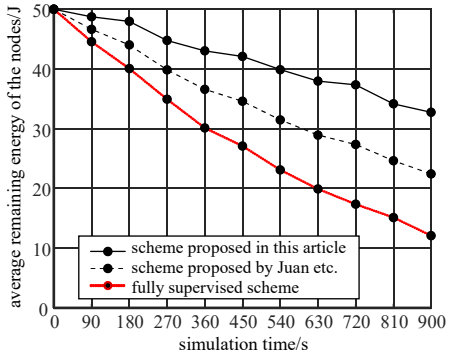


Fig.3 Comparison of node energy consumption

图 3 节点能量消耗对比

在同样的实验环境下重复进行 10 次实验，结果如图 4 所示。Ma[15]等人采用的仅在簇头节点处考虑执行检测的博弈模型检测率在 0.6 至 0.75 之间且十分不稳定。这是由于所有节点都需要依赖簇头节点执行检测，因此簇头节点的能量消耗速度是十分快的。对于某一簇节点而言，当簇头节点因能量耗尽而失效，在切换新的簇头节点的时间片当中，各个节点都是无法执行检测的。而本文提出的基于信息论的博弈方案是将每一个节点都当成一个独立且理性的检测单位，因此检测率在 0.85 以上且变化幅度小，安全性能更稳定。

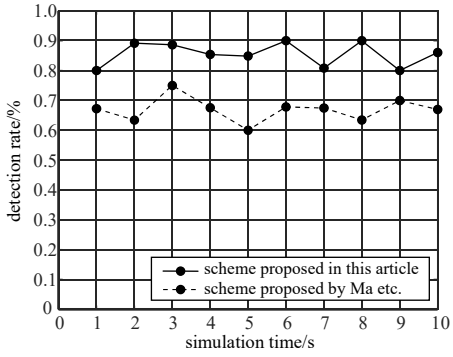


Fig.4 Comparison of scheme accuracy

图 4 方案准确性对比

5 结论

本文结合信息论与博弈论研究了无线传感网中对节点执行检测和监督的开销和系统安全性权衡问题，并且提出了一种基于博弈论的无线传感器网络节点攻防优化模型。详细分析了防守方的防守开销和攻击方的攻击代价，设计攻防双方的效用函数并建立博弈模型。根据信道容量与纳什均衡的融合定理，当博弈达到均衡时双方的效用与博弈信道的信道容量相等，此时双方所采用的行动策略就是博弈的纳什均衡解。实验表明，该模型能够在保障网络安全性需求的前提下有效降低网络能量消耗，延长网络寿命。

参考文献：

[1] RAWAT P,SINGH K D,CHAOUCHI H,et al. Wireless sensor networks: a survey on recent developments and potential synergies[J]. Journal of Supercomputing, 2014, 68(1):68-79.

[2] 崔莉,鞠海玲,苗勇. 无线传感器网络研究进展[J]. 计算机研究与发展, 2005,42(1):163-174. (CUI Li,JU Hailing,MIAO

Yong. Overview of Wireless Sensor Networks[J]. Journal of Computer Research and Development, 2005,42(1):163-174.
[3] MARUTHI S P,PANIGRAHI T,JAGANNATH R P. Distributed version of hybrid swarm intelligence-Nelder Mead algorithm for DOA estimation in WSN[J]. Expert Systems with Applications, 2020,144(1):109-113.
[4] YICK J,MUKHERJEE B,GHOSAL D. Wireless sensor network survey[J]. Computer Networks, 2008,52(12):2292-2330.
[5] MOOSAVI H,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.
[6] ANASTASI G,CONTI M,FRANCESCO M D,et al. Energy conservation in wireless sensor networks: a survey[J]. Ad Hoc Networks, 2009,7(3):537-568.
[7] SHI H Y,WANG W L,KWOK N M,et al. Game theory for wireless sensor networks: a survey[J]. Sensors, 2012,12(12): 9055-9097.
[8] DUAN J,GAO D,YANG D,et al. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications[J]. IEEE Internet of Things Journal, 2014,1(1):58-69.
[9] LI Y,SHI L,CHENG P,et al. Jamming attacks on remote state estimation in cyber-physical systems: a game-theoretic approach[J]. IEEE Transactions on Automatic Control, 2015,60(10):2831-2836.
[10] WALDMAN D E,JENSEN E J. Game theory[M]// Industrial Organization. New York:Addison-Wesley Longman, 2019.
[11] 田有亮,马建峰,彭长根,等. 秘密共享体制的博弈论分析[J]. 电子学报, 2011,39(12):2790-2795. (TIAN Youliang,MA Jianfeng,PENG Changgen,et al. Game-theoretic analysis for the secret sharing scheme[J]. Acta Electronica Sinica, 2011, 39(12):2790-2795.)
[12] MACHADO R,TEKINAY S. A survey of game-theoretic approaches in wireless sensor networks[J]. Computer Networks, 2008,52(16):3047-3061.
[13] AKKARAJITSAKUL K,HOSSAIN E,NIYATO D,et al. Game theoretic approaches for multiple access in wireless networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2011,13(3):372-395.
[14] JUAN P,SANTIAGO Z. Wireless networks under a backoff attack: a game theoretical perspective[J]. Sensors, 2018,18(2):404.
[15] MA Y,CAO H,MA J. The intrusion detection method based on game theory in wireless sensor network[C]// First IEEE International Conference on Ubi-Media Computing. Lanzhou,China:IEEE, 2008.
[16] AHMED A J M A,LIU Yun,ZHANG Zhenjiang,et al. Study on selfish node incentive mechanism with a forward game node in wireless sensor networks[J]. International Journal of Antennas & Propagation, 2017:1-13.
[17] YANG L,LU Y,LIU S,et al. A dynamic behavior monitoring game based trust evaluation scheme for clustering in wireless sensor networks[J]. IEEE Access, 2018,6:71404-71412.
[18] LIAO H,DING S. Mixed and continuous strategy monitor-forward game based selective forwarding solution in WSN[J]. International Journal of Distributed Sensor Networks, 2015(1):1-13.
[19] LAKSHMAN M K. Detecting network intrusions via sampling: a game theoretic approach[C]// IEEE INFOCOM 2003. San Francisco,CA,USA:IEEE, 2003.
[20] CHEN Z,QIAO C,QIU Y,et al. Dynamics stability in wireless sensor networks active defense model[J]. Journal of Computer and System Sciences, 2014,80(8):1534-1548.
[21] QIU Y,CHEN Z,XU L. Active defense model of wireless sensor networks based on evolutionary game theory[C]// International Conference on Wireless Communications Networking & Mobile Computing. Chengdu,China:IEEE, 2010:785-787.
[22] YANG L,LU Y,XIONG L,et al. A game theoretic approach for balancing energy consumption in clustered wireless sensor networks[J]. Sensors, 2017,17(11) :2654.
[23] 林锦锐,李广侠,田世伟. 基于 Stackelberg 博弈的无线定位网络功率分配方案[J]. 太赫兹科学与电子信息学报, 2019,17(6):1006-1011. (LIN Jinrui,LI Guangxia,TIAN Shiwei. Power allocation based on Stackelberg game in wireless location network[J]. Journal of Terahertz Science and Electronic Information Technology, 2019,17(6):1006-1011.)
[24] YANG Y X,NIU X X. The general theory of information security[M]. Beijing:Publishing House of Electronics Industry, 2018.
[25] ABUSAIMEH H,YANG S H. Dynamic cluster head for lifetime efficiency in WSN[J]. International Journal of Automation and Computing, 2009,6(1):48-54.
[26] AGRAWAL D,PANDEY S. FUCA: fuzzy-based unequal clustering algorithm to prolong the lifetime of wireless sensor networks[J]. International Journal of Communication Systems, 2018,31(2):1-18.
[27] GHEORGHE L,RUGHINIS R,NICOLAE T. Energy-efficient authentication and anti-replay security protocol for wireless sensor networks[J]. Control Engineering & Applied Informatics, 2014,16(4):23-27.

(下转第 193 页)