



基于演化博弈的传感节点保密率自适应调节方法^{*}

沈士根^{1,2}, 黄龙军^{1,3}, 屠昂燕^{1,4}, 李宏杰², 韩日昇², 曹奇英⁵

(1. 绍兴文理学院工学院 绍兴 312000;

2. 嘉兴学院数理与信息工程学院 嘉兴 314001;

3. 浙江工业大学计算机科学与技术学院 杭州 310023;

4. 上海大学机电工程与自动化学院 上海 200072;

5. 东华大学计算机科学与技术学院 上海 201620)

摘要:通过扩展经典窃听信道模型,针对聚簇无线传感器网络提出了传感节点和簇头之间的保密率计算方法,构建了一个非合作保密率博弈模型,以反映传感节点之间的交互关系。利用演化博弈思想,建立了传感节点自适应选择发射功率的机制,提出了传感节点自适应调节保密率的算法。实验结果表明,提出的方法能自适应地调节传感节点的保密率,为保证无线传感器网络数据的保密性提供了新途径。

关键词:无线传感器网络;物理层安全;保密率;演化博弈

doi: 10.3969/j.issn.1000-0801.2014.11.013

Secrecy Rate Adaptation Method of Sensor Nodes Based on Evolutionary Game

Shen Shigen^{1,2}, Huang Longjun^{1,3}, Tu Angyan^{1,4}, Li Hongjie², Han Risheng², Cao Qiying⁵

(1. College of Engineering, Shaoxing University, Shaoxing 312000, China;

2. College of Mathematics, Physics and Information Engineering, Jiaxing University, Jiaxing 314001, China;

3. College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China;

4. School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200072, China;

5. College of Computer Science and Technology, Donghua University, Shanghai 201620, China)

Abstract: By developing the classical wire-tap channel, an approach was proposed to compute the secrecy rate between a sensor node and its responsible cluster head in the clustered wireless sensor network. A non-cooperative secrecy rate game model was formulated to reflect on the interaction relationship between sensor nodes. Using evolutionary game theory, a selection scheme in which a power level can be adaptively selected by a sensor node was developed. Moreover, a corresponding algorithm of secrecy rate adaptation was proposed. Numerical experiments show that the proposed algorithm adaptively adjusts the secrecy rate of the sensor node. Therefore, a novel method to guarantee the confidentiality of wireless sensor network data was provided.

Key words: wireless sensor network, physical layer security, secrecy rate, evolutionary game

^{*} 国家自然科学基金资助项目(No.61272034),浙江省自然科学基金资助项目(No.LY13F030012, No.LY13F020035)



1 引言

传感节点资源的有限性决定了保障无线传感器网络(wireless sensor network, WSN)的安全具有很大的挑战性。国内外学者为防御 WSN 中存在的威胁和漏洞,提出了加密机制、攻击检测、安全路由等多种方法^[1]。与传统保障网络通信安全方法不同,物理层安全利用无线信道的物理特性保障无线通信的安全^[2,3]。由于这种方法不需要添加额外组件,而是利用物理层的基础能力实现网络通信安全,所以非常适合资源有限的 WSN。

物理层安全技术的实质是在防止窃听者获得通信数据的同时,最大化源节点到目标节点的可靠通信率(保密率)。其中,最大化的保密率被称为保密容量。Wyner 在其开创性的工作^[4]中介绍了经典窃听模型,并说明了即使不使用密钥也能实现节点间的绝对通信安全。随后,国内外学者对高斯窃听信道^[5]、广播信道^[6]、中继信道^[7]、干扰信道^[8]、MISO (multi-input single-output, 多输入单输出)信道^[9,10]、MIMO (multi-input multi-output, 多输入多输出)信道^[11]等的保密容量进行了系统的基础研究。

当前,已有研究者利用博弈论研究保密容量问题。肖宛阳等人^[12]分析了基于博弈论的物理层安全建模方法。Yuksel 等人^[13]为得到优化的源节点保密率,建立了一种源节点和干扰中继之间的非合作博弈模型。而 Mukherjee 和 Swindlehurst^[14]针对 MIMO 窃听信道模型,通过建立以遍历 MIMO 保密率为支付函数的一个零和博弈,得到了可靠且隐蔽的数据发送策略。Han 等人^[15]利用友好的干扰者干扰窃听者的通信,提高源节点的保密率,建立了一种 Stackelberg 博弈模型,用以反映源节点和友好干扰者的相互关系。Saad^[16]和 Fakoorian^[17]从合作博弈角度,分别引入联盟博弈和 Kalai-Smorodinsky 讨价还价博弈,研究物理层安全问题。

在各种信道保密容量研究基础上,当前的一个焦点问题是如何在相同的网络环境下提高物理层的安全性。然而,现有文献在提高物理层安全性的同时,未考虑对网络通信的影响。实际上,在 WSN 数据通信过程中,发射功率是影响传感节点保密率的关键因素。由于传感节点的自私性,每个传感节点都希望增强自身的发射功率,从而最大化自己的保密率。但这种增强自身发射功率的做法干扰了其他传感节点的通信,同时大大消耗了自身能量。因此,仅考虑最大化传感节点保密率,对整个网络的效用而言不一

定是最优的选择。

本文以最大化网络效用为目标,利用演化博弈方法实现传感节点保密率的自适应调节,该方法在国内外文献中尚未见报道。首先,为适应 WSN 环境扩展了经典保密率计算公式,从而可以深入理解 WSN 中影响保密率的因素;然后,通过建立一种非合作传感节点保密率博弈模型,在解决传感节点力图最大化各自保密率的同时,影响整个网络通信的问题;最后,利用演化博弈论中的复制动力学模型,给出传感节点如何动态地选择各自的发射功率以最大化适应度的演化过程,实现传感节点保密率自适应调节的机制。

2 系统模型

2.1 传感节点干扰模型

本文考虑静态部署的 WSN,即传感节点一旦部署完毕将不再移动。其中,每个传感节点具有唯一的标识,且以节点密度 ρ 部署在二维平面上。每个传感节点配备具有相同增益的发送和接收天线,并以半双工形式工作,即不允许同时发送和接收通信数据。在相同区域内,传感节点的接收和干扰范围主要根据源节点和其他相邻节点的发射功率确定,每个传感节点能根据不同的环境选择不同的发射功率。所有传感节点的部署满足泊松分布规律。

设 r_R 和 r_I 分别是传感节点的接收和干扰距离,则 $r_I \approx 2r_R$ 。通常,一个传感节点的最大干扰节点数由平均的相邻节点数加上 3 倍的标准差 $\sqrt{\sigma}$ 确定。对任何一个传感节点,它的干扰区域 z_I 为 πr_I^2 ,在干扰区域 z_I 中的平均相邻传感节点数为 ρz_I 。在泊松分布中, σ 即 ρz_I 。因此,一个传感节点的最大干扰节点数 I 为:

$$I = \rho z_I + 3\sqrt{\rho z_I} \quad (1)$$

2.2 聚类 WSN 中的传感节点保密率

如图 1 所示,本文研究的 WSN 采用聚类结构。在该结构中,所有传感节点被分成不同的簇。每个簇包括 1 个簇

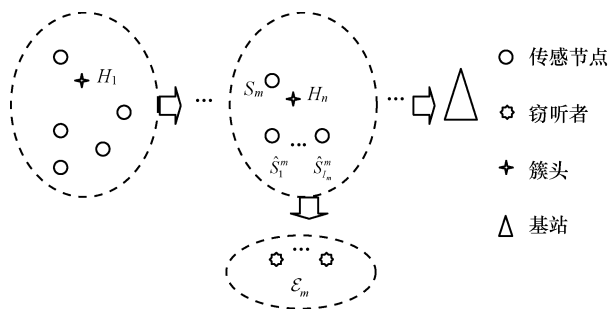


图 1 网络模型

头和若干个传感节点。传感节点捕获数据后首先将数据传输到同一个簇内的簇头,簇头经数据汇聚后再通过其他簇中的簇头将数据传输到基站。需注意的是,本文研究的是一个传感节点与簇头通信时的保密率。

记 $\mathcal{S}=\{S_1, S_2, \dots, S_M\}$, $\mathcal{H}=\{H_1, H_2, \dots, H_N\}$ 和 $\mathcal{E}=\{E_1, E_2, \dots, E_K\}$ 分别为包含 M 个传感节点、 N 个簇头和 K 个窃听者的集合。对 $\forall S_m \in \mathcal{S}$, 存在一个唯一的 $H_n \in \mathcal{H}$, 其中 n 值实质由 m 值确定, 还存在由多个能窃听传感节点 S_m 的窃听器 E_k 组成的集合 $\mathcal{E}_m \subseteq \mathcal{E}$ 。记 $G_{H_n}^{S_m}$ 和 $G_{E_k}^{S_m}$ 分别表示从传感节点 S_m 到簇头 H_n 和窃听器 E_k 的信道增益。为简化模型,假设在簇头端和窃听器端的热噪声功率均为 η^2 , 每个信道的带宽均为 W 。

当多个传感节点同时发送数据时, 将产生信号干扰。对 $\forall S_m \in \mathcal{S}$, 记 $\hat{\mathcal{S}}_m = \{\hat{S}_1^m, \hat{S}_2^m, \dots, \hat{S}_I^m\}$ 为包含 I 个干扰 S_m 信号发送的干扰者, 其中 I 值由式(1)确定。根据经典窃听信道模型计算信道容量的思想可知, 从传感节点 S_m 到对应簇头 H_n 的信道容量 $C_{H_n}^{S_m}$ 为:

$$C_{H_n}^{S_m} = W \lg \left(1 + \frac{P_m G_{H_n}^{S_m}}{\sum_{i=1}^I \hat{P}_i^m G_{H_n}^{\hat{S}_i^m} + \eta^2} \right) \quad (2)$$

其中, P_m 表示传感节点 S_m 选择的发射功率, $\hat{P}_i^m$ 表示干扰节点 $\hat{S}_i^m$ 选择的发射功率, $G_{H_n}^{S_m}$ 表示干扰节点 $\hat{S}_i^m$ 和簇头 H_n 之间的信道增益。

类似地, 从传感节点 S_m 到窃听器 E_k 的信道容量 $G_{E_k}^{S_m}$ 为:

$$C_{E_k}^{S_m} = W \lg \left(1 + \frac{P_m G_{E_k}^{S_m}}{\sum_{i=1}^I \hat{P}_i^m G_{E_k}^{\hat{S}_i^m} + \eta^2} \right) \quad (3)$$

其中, $G_{E_k}^{S_m}$ 表示干扰节点 $\hat{S}_i^m$ 和窃听器 E_k 之间的信道增益。因此传感节点 S_m 和对应簇头 H_n 之间的保密率 $C(P_m)$ 为:

$$C(P_m) = (C_{H_n}^{S_m} - \max_{E_k \in \mathcal{E}_m} C_{E_k}^{S_m})^+ \quad (4)$$

其中, $(x)^+ = \max\{x, 0\}$ 。

3 传感节点保密率的自适应调节机制

3.1 传感节点保密率博弈模型

传感节点保密率博弈模型是一个三元组 $\mathcal{G}(\mathcal{S}, \mathcal{P}, \mathcal{U})$ 。其中, $\mathcal{S}=\{S_1, S_2, \dots, S_M\}$ 表示整个 WSN 中的传感节点集合; $\mathcal{P} = \prod_{m=1}^M \mathcal{P}_m$ 表示所有传感节点可选择功率策略的集合,

$\mathcal{P}_m = \{P_m | P_1^m, P_2^m, \dots, P_L^m\}$ 为传感节点 S_m 可选择的功率策略 $\mathcal{P}_m$ 的集合, L 表示 S_m 可选择的功率策略的个数; $\mathcal{U} = \{\mu(P_m, P_{\tilde{m}}) | P_m \in \mathcal{P}_m, P_{\tilde{m}} \in \mathcal{P}_{\tilde{m}}, m, \tilde{m} \in \{1, 2, \dots, M\}\}$ 表示传感节点 S_m 选择功率策略 P_m , 且它的对手选择功率策略 $P_{\tilde{m}}$ 时的效用集合。

根据演化博弈论的观点, 可将集合 $\mathcal{S}$ 中的所有传感节点看作一个种群 (population), 每个传感节点对应种群中的一个个体。这些个体能根据它们当前的适应度 (即期望效用) 自动调节各自的策略。也就是说, 通过最大化传感节点的适应度自适应调节各自的保密率。

为反映传感节点在增大发射功率时提高自身保密率, 同时增大自身能量消耗和干扰其他节点的实际情况, 定义传感节点的效用函数 $\mu(P_m, P_{\tilde{m}})$ 为:

$$\mu(P_m, P_{\tilde{m}}) = C(P_m) - \alpha P_m \quad (5)$$

其中, $C(P_m)$ 由式(4)确定, α 是一个用于反映传感节点在发送数据时消耗能量状况的成本参数。值得注意的是, 选择发射功率 P_m 的干扰节点对传感节点 S_m 的影响已体现在 $C(P_m)$ 中。

3.2 传感节点保密率的动力学分析

本文利用演化博弈论中的复制动力学分析传感节点保密率的变化过程。所有传感节点开始时从各自可用的功率集合中随机选择一种发射功率用于发送通信数据。由于每个传感节点都希望最大化各自的适应度, 所以它们会与 WSN 的平均适应度进行比较, 调节自身的发射功率, 即调节自身的保密率。当整个 WSN 的平均适应度高于传感节点自身的适应度时, 它们通过改变自身的发射功率, 改变自身的适应度; 否则, 保持原来的发射功率。记 $\theta_j(t)$ 为阶段 t 选择功率策略 j 的传感节点在整个 WSN 中所占的比例, 则有:

$$\sum_{j \in \mathcal{P}_m} \theta_j(t) = 1 \quad (6)$$

整个的状态 $\theta(t)$ 可表示为 $[\theta_{P_1^m}(t), \theta_{P_2^m}(t), \dots, \theta_{P_L^m}(t)]$, 可看作整个 WSN 的混和策略。记 l 为传感节点 S_m 的对手 $S_{\tilde{m}}$ 选择的功率策略。根据参考文献[18]可得, 传感节点 S_m 在阶段 t 选择功率策略 j 的适应度 $\mu_j(t)$ 为:

$$\mu_j(t) = \sum_{l \in \mathcal{P}_{\tilde{m}}} \theta_l(t) \mu(j, l) \quad (7)$$

其中, $\mu(j, l)$ 由式(5)确定。整个 WSN 在阶段 t 的平均适应度 $\bar{\mu}(t)$ 为:

$$\bar{\mu}(t) = \sum_{j \in \mathcal{P}_m} \theta_j(t) \mu_j(t) \quad (8)$$



相应地,可定义传感节点 S_m 在阶段 t 选择功率策略 j 的期望保密率 $\zeta_j(t)$ 为:

$$\zeta_j(t) = \sum_{l \in \mathcal{P}_m} \theta_l(t) C(j) \quad (9)$$

其中, $C(j)$ 由式(4)确定。整个 WSN 在阶段的平均期望保密率 $\bar{\zeta}(t)$ 为:

$$\bar{\zeta}(t) = \sum_{j \in \mathcal{P}_m} \theta_j(t) \zeta_j(t) \quad (10)$$

下面分析传感节点的策略改变率。记 $r_j(\theta)$ 为选择功率策略 j 的传感节点的平均策略改变率, $p_q^j(\theta)$ 为传感节点改变当前功率策略 j 到 q 的概率, 则整个 WSN 中改变功率策略 j 到 q 的传感节点所占比例为 $\theta_j(t) r_j(\theta) p_q^j(\theta)$ 。因此, 从功率策略 j 转换为其他功率策略的传感节点转出总比例为:

$$\begin{aligned} \sum_{q, q \neq j} \theta_j(t) r_j(\theta) p_q^j(\theta) &= \theta_j(t) r_j(\theta) \sum_{q, q \neq j} p_q^j(\theta) \\ &= \theta_j(t) r_j(\theta) (1 - p_j^j(\theta)) \end{aligned} \quad (11)$$

从其他功率策略转换到功率策略 j 的传感节点转入总比例为 $\sum_{q, q \neq j} \theta_q(t) r_q(\theta) p_j^q(\theta)$ 。

至此, 将选择功率策略 j 的传感节点转入总比例减去转出总比例, 可得到整个 WSN 中选择功率策略 j 的传感节点比例变化的动力学方程为:

$$\begin{aligned} \dot{\theta}_j(t) &= \sum_{q, q \neq j} \theta_q(t) r_q(\theta) p_j^q(\theta) - \theta_j(t) r_j(\theta) (1 - p_j^j(\theta)) \\ &= \sum_q \theta_q(t) r_q(\theta) p_j^q(\theta) - \theta_j(t) r_j(\theta) \end{aligned} \quad (12)$$

式(12)中的 $p_j^q(\theta)$ 决定于选择功率策略 j 和 q 的适应度 $\mu_j(t)$ 和 $\mu_q(t)$ 。只有当 $\mu_q(t) > \mu_j(t)$, 传感节点才会从功率策略 j 改变为 q 。因此, 存在一个连续可微的概率分布函数 $\phi: \mathbb{R} \rightarrow [0, 1]$, 使得:

$$p_j^q(\theta) = \begin{cases} \phi(\mu_q(t) - \mu_j(t)), & q \neq j \\ 1 - \sum_{q \neq j} \phi(\mu_q(t) - \mu_j(t)), & q = j \end{cases} \quad (13)$$

为简化分析过程, 令所有传感节点的平均策略改变率恒等于 1, 即:

$$\forall j \in \mathcal{P}_m, r_j(\theta) \equiv 1 \quad (14)$$

将式(13)和式(14)代入式(12), 则整个 WSN 中选择功率策略 j 的传感节点比例变化的动力学方程为:

$$\dot{\theta}_j(t) = \theta_j(t) \sum_{q, q \neq j} \theta_q(t) (\phi(\mu_j(t) - \mu_q(t)) - \phi(\mu_q(t) - \mu_j(t))) \quad (15)$$

根据参考文献[19]中线性化函数 ϕ 的思想, 可设:

$$\phi(x) = \beta + \gamma x \quad (16)$$

其中, $\beta, \gamma \in \mathbb{R}$ 且 $0 \leq \beta + \gamma x \leq 1$ 。将式(16)代入式(15), 得到整个 WSN 中选择功率策略 j 的传感节点比例变化的动力学方程为:

$$\dot{\theta}_j(t) = 2\gamma \theta_j(t) \sum_{q, q \neq j} \theta_q(t) (\mu_j(t) - \mu_q(t)) \quad (17)$$

其中, γ 是一个影响整个 WSN 达到演化稳定策略收敛速度的参数。

3.3 传感节点保密率自适应调节算法

在每个传感节点自适应调节各自保密率的过程中, 首先计算各自当前的适应度, 然后再与整个 WSN 的平均适应度进行比较。若差值大于一个给定的上限值, 则根据式(17)选择新的功率策略。反复进行该过程, 直到整个 WSN 达到演化稳定状态, 此时每个传感节点选择的功率策略为演化稳定策略, 对应最优的网络效用。在整个演化过程中, 传感节点通过自适应改变选择的功率策略实现保密率的自适应调节。传感节点保密率自适应调节算法的具体过程如下。

步骤 1 初始化 W, I, η^2 和信道增益等所有参数, $t \leftarrow 0$ 。

步骤 2 以概率 $\theta(t) = [1/L, 1/L, \dots, 1/L]$ 选择一种功率策略 j , 这种“等概率”的选择可以保证传感节点保密率博弈开始时每个传感节点具有相同的适应度。

步骤 3 根据式(7)和式(8)分别计算传感节点选择功率策略 j 的适应度 $\mu_j(t)$ 和整个 WSN 的平均适应度 $\bar{\mu}(t)$ 。

步骤 4 根据式(9)和式(10)分别计算传感节点选择功率策略 j 的期望保密率 $\zeta_j(t)$ 和整个 WSN 的平均期望保密率 $\bar{\zeta}(t)$ 。

步骤 5 Do While

If $|\bar{\mu}(t) - \mu_j(t)| < \tau$ // τ 表示一个给定的下限值

Exit;

End If

If $|\bar{\mu}(t) - \mu_j(t)| > \tilde{\tau}$ // $\tilde{\tau}$ 表示一个给定的下限值

根据式(17)计算功率选择概率 $\theta(t+1)$;

以 $\theta(t+1)$ 选择一个新的功率策略 j ;

根据式(7)和式(8)分别计算传感节点选择功率策略 j 的适应度 $\mu_j(t+1)$ 和整个 WSN 的平均适应度 $\bar{\mu}(t+1)$;

根据式(9)和式(10)分别计算传感节点选择功率策略 j 的期望保密率 $\zeta_j(t+1)$ 和整个 WSN 的平均期望保密率 $\bar{\zeta}(t+1)$;

End If

$t \leftarrow t+1$

End Do;

步骤 6 返回数组 ζ_j 和 $\bar{\zeta}$ 。

4 实验仿真

由于传感节点在计算能力、存储能力和能量等方面具有局限性,实验过程中假设每个传感节点在保密率博弈过程中能选择的功率策略集合仅包含两个策略。也就是说,对 $\forall S_m, P_m = \{P_H, P_L\}$, 其中 P_H 和 P_L 分别表示高功率策略和低功率策略。

传感节点保密率博弈模型中的参数根据 IEEE 802.15.4 物理层规范进行设置。其中, $\rho=0.01$, $W=2$ MHz, $P_H=30$ mW, $P_L=10$ mW, $\sigma^2=-112$ dBm, $G_{H_m}^S=1$, $G_{L_m}^S=0.6$ 。由于传感节点选择的功率越大,产生的干扰范围越大,因此分别设置 $r_H=50$ m 和 $r_L=10$ m, r_H 和 r_L 分别表示传感节点选择功率策略 P_H 和 P_L 产生的干扰半径。另外,根据经验值假设干扰者的工作概率为 0.01。这样结合式(1),可得到选择功率策略 P_H 和 P_L 的干扰节点数量分别为 $0.01 \times (\rho \pi r_H^2 + 3 \sqrt{\rho \pi r_H^2})$ 和 $0.01 \times (\rho \pi r_L^2 + 3 \sqrt{\rho \pi r_L^2})$ 。

为方便描述,记 $\theta_H(t)$ 为整个 WSN 中传感节点在阶段 t 选择功率策略 P_H 所占的比例,则整个 WSN 中传感节点在阶段 t 选择功率策略 P_L 所占的比例为 $1-\theta_H(t)$ 。由式(7)可得,传感节点在阶段 t 选择功率策略 P_H 和 P_L 的适应度 $\mu_H(t)$ 和 $\mu_L(t)$ 分别为:

$$\mu_H(t) = \theta_H(t)\mu(P_H, P_H) + (1-\theta_H(t))\mu(P_H, P_L) \quad (18)$$

$$\mu_L(t) = \theta_H(t)\mu(P_L, P_H) + (1-\theta_H(t))\mu(P_L, P_L) \quad (19)$$

由式(8)可得,整个 WSN 在阶段 t 的平均适应度 $\bar{\mu}(t)$ 为:

$$\bar{\mu}(t) = \theta_H(t)\mu_H(t) + (1-\theta_H(t))\mu_L(t) \quad (20)$$

由式(9)可得,传感节点在阶段 t 选择功率策略 P_H 和 P_L 的期望保密率 $\zeta_H(t)$ 和 $\zeta_L(t)$ 分别为:

$$\zeta_H(t) = \theta_H(t)\zeta_{HH} + (1-\theta_H(t))\zeta_{HL} \quad (21)$$

$$\zeta_L(t) = \theta_H(t)\zeta_{LH} + (1-\theta_H(t))\zeta_{LL} \quad (22)$$

对 $\forall u, v \in \{H, L\}$, ζ_{uv} 表示当干扰节点选择功率策略 P_v 时,一个选择功率策略 P_u 的传感节点的保密率,其值由式(4)计算得到。由式(10)可得,整个 WSN 在阶段 t 的平均期望保密率 $\bar{\zeta}(t)$ 为:

$$\bar{\zeta}(t) = \theta_H(t)\zeta_H(t) + (1-\theta_H(t))\zeta_L(t) \quad (23)$$

图 2 和图 3 给出了当成本参数 α 值为 3 时,传感节点

采用保密率自适应调节算法的调节过程。在图 2 中, P_H 是传感节点保密率博弈模型的演化稳定策略。从图 2 可以看出,即使最初选择功率策略 P_H 的比例只有 0.5%,当 t 值大于 40 后, $\theta_H(t)$ 趋向于稳定值 1。这意味着传感节点选择功率策略 P_H 的适应度总是高于选择 P_L 的适应度,因此所有的传感节点经过自适应调节,最终均选择 P_H 作为自己的功率策略。此时, $\zeta_H(t)$, $\zeta_L(t)$ 和 $\bar{\zeta}(t)$ 收敛后的极限值分别约为 132.997 6、48.447 4 和 132.914 8,如图 3 所示。

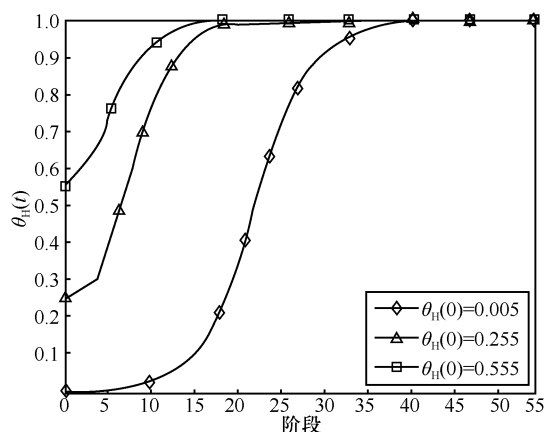


图 2 $\alpha=3$ 时 $\theta_H(t)$ 的演化趋势

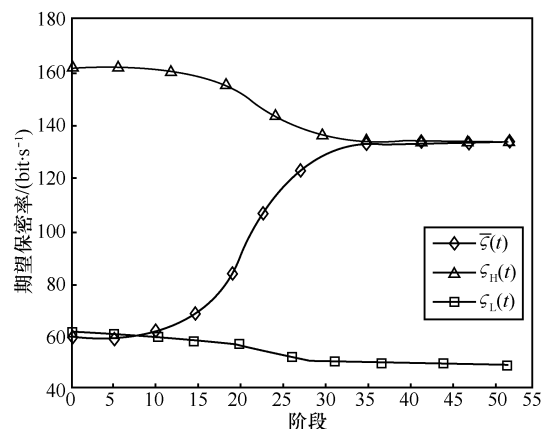


图 3 $\alpha=3$ 时期望保密率的演化趋势

图 4 和图 5 给出了当成本参数 α 值为 4.5 时,传感节点采用保密率自适应调节算法的调节过程。在图 4 中,传感节点保密率博弈模型存在一个值约为 (0.684 1, 0.315 8) 的演化稳定混合策略。达到该均衡点意味着约 68.41% 的传感节点选择 P_H , 而约 31.58% 的传感节点选择 P_L 。此时,传感节点选择 P_H 或 P_L 具有相同的适应度,但从图 5 可以看出, $\zeta_H(t)$, $\zeta_L(t)$ 和 $\bar{\zeta}(t)$ 收敛后的极限值分别约为 141.830 9、51.830 9 和 113.394 9。这说明虽然选择功率策略 P_H 的期望保密率值高,但并非所有的传感节点都选择 P_H 作为自身的功率策略。

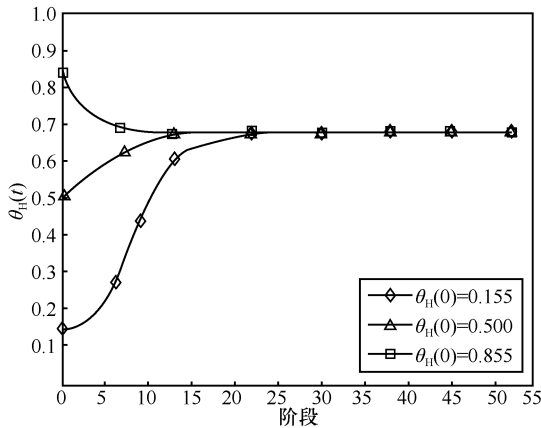
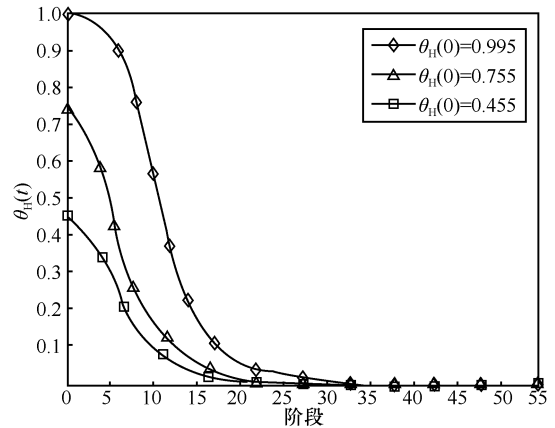
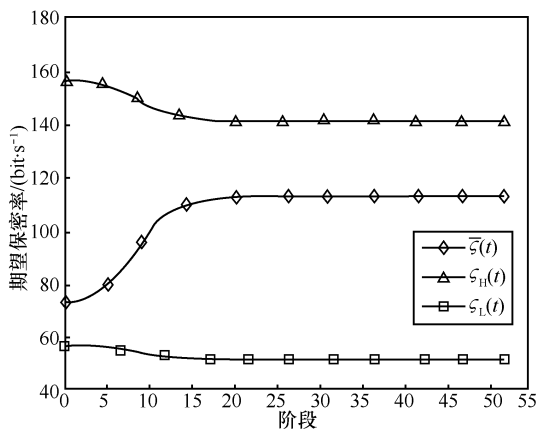
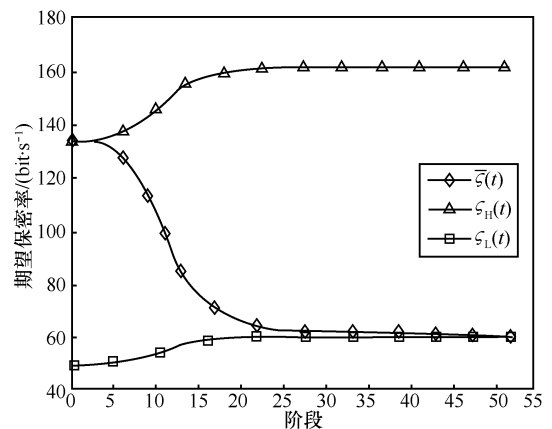
图4 $\alpha=4.5$ 时 $\theta_H(t)$ 的演化趋势图6 $\alpha=6$ 时 $\theta_H(t)$ 的演化趋势图5 $\alpha=4.5$ 时期望保密率的演化趋势图7 $\alpha=6$ 时期望保密率的演化趋势

图6和图7给出了当成本参数 α 值为6时,传感节点采用保密率自适应调节算法的调节过程。在图6中, P_L 是传感节点保密率博弈模型的演化稳定策略。从图6中可以看出,即使最初选择功率策略 P_H 的比例达到99.5%,当 t 值大于30后, $\theta_H(t)$ 趋向于稳定值0。这意味着传感节点选择 P_L 的适应度总是高于选择 P_H 的适应度,因此所有的传感节点经过自适应调节,最终均选择 P_L 作为自己的功率策略。此时, $\zeta_H(t)$ 、 $\zeta_L(t)$ 和 $\bar{\zeta}(t)$ 收敛后的极限值分别约为161.013 8、59.178 9和59.199 4,如图7所示。这说明虽然选择功率策略 P_H 的期望保密率值高,但所有的传感节点仍选择 P_L 作为自身的功率策略。

5 结束语

本文基于经典窃听信道模型扩展的保密率可适应聚簇WSN环境,构建的传感节点保密率博弈模型能反映传感节点的交互过程。基于演化博弈论中复制动力学原理的传感节点比例变化动力学方程,能使传感节点根据自身当

前的适应度和WSN的平均适应度,动态选择自身的功率策略,是一种自适应调节传感节点保密率的方法。实验进一步阐明了该方法的机理,为利用物理层安全技术保证WSN数据的保密性,提供了新途径。

参考文献

- 1 Chen X, Makki K, Yen K, *et al.* Sensor network security: a survey. *IEEE Communications Surveys & Tutorials*, 2009, 11(2): 52~73
- 2 Poor H V. Information and inference in the wireless physical layer. *IEEE Wireless Communications*, 2012, 19(1): 40~47
- 3 龙航, 袁广翔, 王静等. 物理层安全技术研究现状与展望. *电信科学*, 2011, 27(9): 60~65
- 4 Wyner A D. The wire-tap channel. *Bell System Technical Journal*, 1975, 54(8): 1355~1387
- 5 Leung-Yan-Cheong S K, Hellman M E. The Gaussian wire-tap channel. *IEEE Transactions on Information Theory*, 1978, IT-24(4): 451~456
- 6 Csiszár I, Körner J. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 1978, IT-24(3): 339~348

- 7 Awan Z H, Zaidi A, Vandendorpe L. Secure communication over parallel relay channel. *IEEE Transactions on Information Forensics and Security*, 2012, 7(2): 359~371
- 8 Liu R, Marić I, Spasojević P, *et al.* Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions. *IEEE Transactions on Information Theory*, 2008, 54(6): 2493~2507
- 9 吉江, 金梁, 黄开枝. 基于人工噪声的 MISO 保密容量分析. *通信学报*, 2012, 33(10): 138~142
- 10 Gerbracht S, Scheunert C, Jorswieck E A. Secrecy outage in MISO systems with partial channel information. *IEEE Transactions on Information Forensics and Security*, 2012, 7(2): 704~716
- 11 Shafiee S, Liu N, Ulukus S. Towards the secrecy capacity of the gaussian MIMO wire-tap channel: the 2-2-1 channel. *IEEE Transactions on Information Theory*, 2009, 55(9): 4033~4039
- 12 肖宛阳, 黄开枝, 罗兴国等. 基于博弈论的物理层安全建模及现状分析. *信息工程大学学报*, 2013, 14(4): 402~409
- 13 Yuksel M, Liu X, Erkip E. A secure communication game with a relay helping the eavesdropper. *IEEE Transactions on Information Forensics and Security*, 2011, 6(3): 818~830
- 14 Mukherjee A, Swindlehurst A L. Jamming games in the MIMO wiretap channel with an active eavesdropper. *IEEE Transactions on Signal Processing*, 2013, 61(1): 82~91
- 15 Han Z, Marina N, Debbah M, *et al.* Physical layer security game: interaction between source, eavesdropper, and friendly jammer. *Eurasip Journal on Wireless Communications and Networking*, 2009:1~10
- 16 Saad W, Han Z, Başar T, *et al.* Distributed coalition formation games for secure wireless transmission. *Mobile Networks and Applications*, 2011, 16(2): 231~245
- 17 Fakoorian S A A, Swindlehurst A L. MIMO interference channel with confidential messages: achievable secrecy rates and precoder design. *IEEE Transactions on Information Forensics and Security*, 2011, 6(3): 640~649
- 18 Fudenberg D, Levine D K. *The Theory of Learning in Games*. Cambridge: MIT Press, 1998
- 19 Weibull J W. *Evolutionary Game Theory*. Cambridge: MIT Press, 1995

[作者简介]



沈士根,男,博士,绍兴文理学院工学院教授,主要研究方向为无线传感器网络、博弈论。

黄龙军,男,浙江工业大学计算机科学与技术学院博士生,绍兴文理学院工学院讲师,主要研究方向为无线传感器网络、博弈论。

屠昂燕,女,上海大学机电工程与自动化学院博士生,绍兴文理学院工学院讲师,主要研究方向为无线传感器网络、网络调度和优化。

李宏杰,男,博士,嘉兴学院数理与信息工程学院副教授,主要研究方向为复杂网络、优化控制。

韩日昇,男,博士,嘉兴学院数理与信息工程学院讲师,主要研究方向为复杂网络、优化控制。

曹奇英,男,博士,东华大学计算机科学与技术学院教授,主要研究方向为普适计算、智能信息处理。

(收稿日期:2014-07-09)

• 简讯 •

声 明

读者来信反映,我刊 2013 年 12 期上发表的《无线传感器网络数据自适应稀疏变换》(作者:浙江工业职业技术学院 陈暄)不属国家自然科学基金项目(No.61273072)资助论文。经与该项目负责人杭州电子科技大学蒋鹏老师确认,该文稿所述工作及作者陈暄与此项目没有任何关联,系作者陈暄擅自盗用国家自然科学基金项目名称。对此学术不端行为,编辑部特此撤销该文稿在相关合作数据库的检索,并予以谴责!

希望广大作者重视学术道德和行为规范,加强自律。我们也将加强对录用文稿涉及学术不端的审查,进一步保障发表文稿的学术质量。

《电信科学》编辑部

2014 年 11 月