针对窃听问题的马尔可夫博弈路由模型的研究

马争先 董荣胜 王玉斌 刘建明
(桂林电子科技大学计算机科学与工程学院 桂林 541004)

摘 要 在随机路由的基础上,给出一种针对窃听问题的马尔可夫博弈路由模型(Markov Game Theory-based Routing,MGBR)。给出的模型以发送者和窃听者为马尔可夫博弈双方,发送者通过概率进行数据传输,增加了窃听者窃听信息的难度。模型通过收益函数计算纳什均衡点,找出最优路径。使用PRISM工具进行仿真,结果表明MGBR中存在纳什均衡点,在纳什均衡点处信息被窃听的概率最小;给出信息在纳什均衡点处被窃听的概率变化趋势,与基于最小跳数算法的路由协议相比,它降低了信息被窃听的概率。

关键词 无线传感器网络,马尔可夫博弈路由模型,概率
中图法分类号 TP393.08 **文献标识码** A

Markov Game Theory Based Routing Countering Eavesdropping

MA Zheng-xian DONG Rong-sheng WANG Yu-bin LIU Jian-ming
(School of Computer and Control,Guilin University of Electronic Technology,Guilin 541004,China)

Abstract To reduce the probability of eavesdropping in wireless sensor networks,this paper proposed a Markov game theory based routing(MGBR) to counter tapping problems under stochastic routing. The sender and the eavesdropper are considered as the two players of the game. Data is transmitted by senders with probability,determining the data transmission to effective tap is hence difficult for the eavesdroppers. With the tool of PRISM,simulation results demonstrate that there is a Nash Equilibrium point in MGBR,where the probability to be eavesdropped can be minimized. Furthermore,we presented the probability variation tendency of information to be eavesdropped on the Nash Equilibrium point. Compared with protocol based on minimal-hop algorithm,MGBR can reduce the probability of information to be eavesdropped effectively.

Keywords WSN,MGBR,Probability

无线传感器网络(Wireless Sensor Networks,WSN)路由有3种方式:直接通讯[1]、平面路由[2,3]和层次路由[4,5]。不少学者对WSN路由进行了研究。徐许亮等针对节点之间的协作,给出了两种博弈模型[6,7]。曾加等[8]针对WSN能耗不均问题,提出了一种基于博弈论模型的能量平衡路由。汪洋等[9]针对无线环境中自私节点进行了基于非合作博弈理论的路由机制的分析和研究。Qui等人[10]针对自私路由给出了博弈模型,在类网络环境(Internet-like environments)中,通过路由策略,使自私路由接近最优平均等待时间。R. La和V. Anantharam[11]在自私用户的通讯网络上建立了重复博弈模型,用一个折扣因子来重复博弈,并研究得出了纳什均衡点花费不大于阶段博弈的花费。R. Kannan等人[12]在传感器网络的一组节点上建立一个路由树,把问题公式化为一个非零和博弈。在该博弈中,每个节点均为一个博弈者,为了最大化估计点对点路径的可能性而独立决定下一跳,这种可能性将减少下一跳的通讯花费。S. Bohacek等人[13]提出了基于博弈论的随机路由,给出了Online game和Offline game两种博弈模型,针对节点攻击,给出两种博弈策略,使连接和路由故障最小化。

上述论文研究的路由模型均未涉及窃听问题。本文针对WSN中窃听问题,给出了基于马尔可夫博弈的路由(MGBR)模型。使用混合策略,计算收益函数,找出MGBR的纳什均衡点,使用PRISM工具进行试验仿真,结果表明MGBR模型可降低数据被窃听的概率。

1 马尔可夫博弈

马尔可夫博弈(Markov Game)也称随机博弈,是一种包含一个或多个参与者进行的具有状态概率转移的动态博弈过程。

定义1 马尔可夫博弈可形式化为一个五元组 $M=(a,S,A,P,R)$。其中:

1) a 是博弈者的集合;

2) S 是状态集;

3) A 是联合行为空间,博弈者 i 的可用行为集表示为 A_i;

4) P 是状态转移概率函数;

5) R 表示收益函数,博弈者 i 的收益函数表示为 $R_i:A_1\times$

到稿日期:2010-12-30 返修日期:2011-03-24 本文受国家自然科学基金项目(60762002),广西自然科学基金项目(0991242)资助。
马争先(1983—),男,硕士生,主要研究方向为无线传感器网络性能;董荣胜(1965—),男,教授,主要研究方向为协议工程;王玉斌(1984—),男,硕士生,主要研究方向为无线传感器网络安全;刘建明(1975—),男,博士,副教授,主要研究方向为无线通信网络、排队理论等。

$A_2 \times \cdots \times A_n \to R$。

马尔可夫博弈由多个博弈阶段组成。参与者选择自身的策略并获得由当前状态和策略决定的报酬。博弈按照概率的分布和参与者策略随机转移到下一个阶段。在新的状态阶段，重复上一次的策略选择过程，博弈继续进行。通过计算各个阶段报酬的贴现值或报酬平均值的下限来表示参与者在随机博弈中获得的全部报酬。

在 WSN 中，传输的信息很可能被窃听。若窃听者具有记忆功能，将给后续数据的传输带来不安全因素。此外，节点数据的传输只与目前节点和节点采取的行动有关，该行为被称为马尔可夫性，因此可以构建 WSN 路由的马尔可夫博弈模型，以便于 WSN 性能的研究。

2 MGBR 模型

2.1 MGBR 的形式定义

MGBR 模型中，假设网络每条路径所涉节点个数为 N，N_i，N_j 分别表示第 i，j 个节点，$1 \leqslant i, j \leqslant N$。马尔可夫博弈路由模型定义为：

$\Gamma = (A, S, M, P, R)$

其中：

1）A 为博弈者的集合，a_s 和 a_a 为 A 的两个元素 $a_s \in A$，$a_a \in A$，分别表示数据发送者和窃听者；

2）S 为状态集，即各个阶段下发送节点与窃听者的组合状态 $S_1, S_2, \cdots, S_N, S_i (1 \leqslant i \leqslant N)$，表示节点 i 上，a_s 发送数据的同时 a_a 也采取相应的窃听策略，即二者的联合状态；

3）M 为行为空间集合，是 a_s 与 a_a 行为动作集合，$M = \begin{pmatrix} m_{s\bar{a}} & m_{sa} \\ m_{\bar{s}\bar{a}} & m_{\bar{s}a} \end{pmatrix}$

①$m_{s\bar{a}}$ 表示发送者未发送数据且窃听者未窃听的行为；

②m_{sa} 表示发送者未发送数据且窃听者窃听的行为；

③$m_{\bar{s}\bar{a}}$ 表示发送者发送数据且窃听者未窃听的行为；

④$m_{\bar{s}a}$ 表示发送者发送数据且窃听者窃听的行为；

4）P 为状态转移概率函数，表示发送者从状态 S 到状态 S' 的概率，对应着行为空间，概率也分为 4 种：$P = \begin{pmatrix} p_{s\bar{a}} & p_{sa} \\ p_{\bar{s}\bar{a}} & p_{\bar{s}a} \end{pmatrix}$，它们分别表示未发送未窃听、未发送窃听、发送未窃听、发送窃听的概率；

5）R 为收益函数，R_s 表示状态发送者（a_s）的收益函数，R_a 表示状态窃听者（a_a）的收益函数，且 $R_s \in R$，$R_a \in R$。

2.2 概率有限状态自动机

MGBR 模型中的状态转移可以由概率有限状态自动机表示，$M = (Q, \Sigma, \delta, q_0, F)$，$M$ 中的各个元素描述如下：

1）Q 是状态的非空有限集合，q 是 Q 的任一状态；

2）Σ 是输入，定义为空，也就是不需要输入，状态转移只与随概率的变化有关；

3）δ 为状态概率转移函数，$\delta: Q \times \Sigma \to Q'$，状态通过概率转移函数进入新的状态，$0 < \delta \leqslant 1$；

4）q_0 是 M 的初始状态，$q_0 \in Q$；

5）F 是 M 的终止状态集合，$F \subseteq Q$，在此有限状态自动机其终止状态 $F = \{q_{s\bar{a}}, q_{sa}, q_{\bar{s}\bar{a}}, q_{\bar{s}a}\}$，$q_{s\bar{a}}, q_{sa}, q_{\bar{s}\bar{a}}, q_{\bar{s}a} \in Q$ 分别表示未发送未窃听、未发送窃听、发送未窃听、发送窃听的状态。

状态转移图如图 1 所示，图中，$\alpha, \beta, \gamma, \cdots$ 是转移概率，$\sum q_i = 1$ 且 $i \in \{\alpha, \beta, \gamma, \cdots\}$。

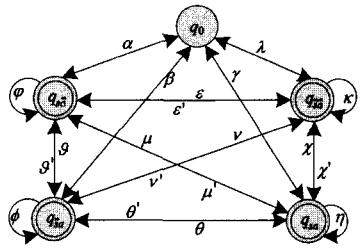

图 1 状态转移图

2.3 节点传输

在 WSN 中，汇聚节点把普通节点的信息进行汇聚、提取并转发。图 2 中，假设节点 10 向节点 9 发送数据。

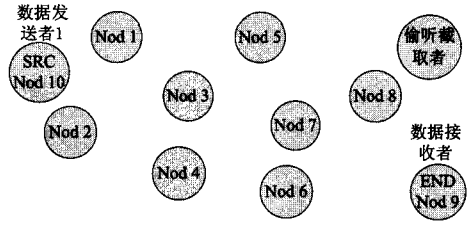

图 2 随机分布的节点图

在 MGBR 模型中，数据的传输是源节点向目的节点发送数据的过程，发送者或转发者与窃听者之间进行博弈。另外，该博弈更侧重于拥有数据的节点和此节点所采取的策略，与先前的状态没有关系。当节点的信息传送到下一节点时，下一节点成为新的发送者，重新采取策略进行数据的发送，直至目的节点。如图 2 所示，数据传输过程中，约定：

1）定义源节点不接受任何数据，只向外发送数据；

2）节点在通讯范围内进行数据的传输，只向目的节点近的节点传送数据，而不进行偏离目的节点的数据传输；

3）目的节点定义为吸收态，数据到达吸收态后将不再传输；

4）远离目的节点的传输的概率为 0，例如图中如果节点 9 是目的节点，数据传输到节点 8，它将不再向节点 5 传输；

5）目的节点的邻节点向目的节点传输的概率为 1，不再向比本身节点近的节点发送；

6）节点向外传输的概率和为 1，$\sum_{i=C} P_{Si \to j} = 1$；窃听者向可能传输节点的概率和也为 1，$\sum_{i=C} P_{Ai \to m} = 1$；

7）惩罚函数，发送者每经过一个节点，$R_s = -K$，否则为 0；窃听者每经过一个节点，R_a 为 K，否则为 0；

8）节点之间的转发概率可以根据跳数、能量等以及惩罚值来确定；

9）发送者每个阶段采用的途径集合空间为 S_ℓ，窃听者采用的路径集合空间为 A_ℓ。

给出了节点的转移概率，如图 3 所示。

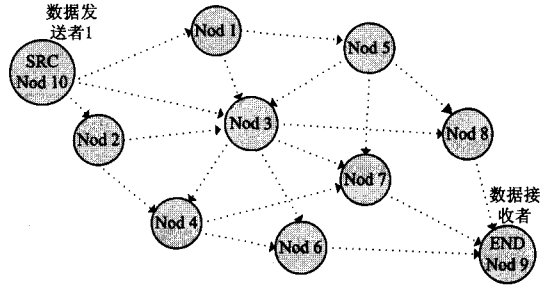

图 3 节点的概率转移

根据上述约定，传输过程无回路问题，传输过程无死循环，有助于数据的顺利传输。

马尔可夫博弈是一种特殊的重复博弈，每个博弈阶段需要重新定义博弈状态。初始博弈状态如图 4 所示。

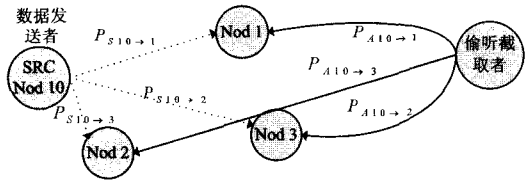

图 4　第一发送状态

在此过程中节点 10 将会以概率 $P_{s10\to1}$，$P_{s10\to2}$，$P_{s10\to3}$ 向节点 1,2,3 发送数据，同时窃听者也会以概率的形式进行节点的选择，从而完成对数据的窃听。在此阶段结束后，数据将进入下一阶段的博弈，如果数据选择节点 3，下一阶段的转发形式如图 5 所示。阶段博弈将以此类推，直至数据发送完成。

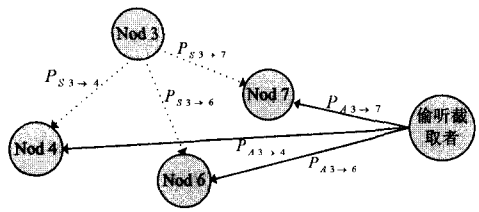

图 5　模型状态

3　MGBR 模型的概率

3.1　发送者的概率

若惩罚函数为 0，则节点对下一跳各节点的选择概率相等，$P_{K\to i}=1/W$（节点 K 对下一跳的个数为 W）；若惩罚函数不为 0，则需定义补偿概率 $\delta_{k\to i}$。所以通过补偿后的概率为：

$$P'=P_{K\to i}+\delta_{k\to i} \tag{1}$$

$$\delta_{k\to i}=(E(\bar{\omega}_i)-\bar{\omega}_i)/\sum\bar{\omega}_i \tag{2}$$

$$E(\bar{\omega}_i)=\sum P_{K\to i}\bar{\omega}_{i'} \tag{3}$$

式中，$\bar{\omega}_i$ 是概率变化前的节点 K 到目的节点的期望跳数。

使用逆推迭代计算 $\bar{\omega}_i$ 的值。先计算出离目的节点最近的 $\bar{\omega}$ 值，然后依次迭代出离源节点最近的 $\bar{\omega}$ 值。$\bar{\omega}$ 的值随博弈阶段的变化而改变。若惩罚函数的值定义得较大，一次惩罚将不能满足要求，可以定义二次惩罚或多次惩罚，并迭代出 $\bar{\omega}$ 的值。迭代公式如式(2)所示。

3.2　窃听者的概率

窃听者根据节点的分布来进行概率的调整，初始条件下窃听概率相等。然后根据跳数进行概率补偿。其补偿概率为 δ'，它与发送者的概率补偿具有相同的形式，但是它的数值不同，计算公式如下：

$$\delta'=\delta/\sum_i\sum_j P_{Si\to j} \tag{4}$$

4　路由策略

在 MGBR 模型中，发送者和窃听者的期望值分别为：

$$E_S=\sum_{i\in\Omega}\sum_{j\in\Psi}P_{Si\to j}R_{Si\to j} \tag{5}$$

$$E_A=\sum_{i\in\Omega}\sum_{j\in\Psi}P_{Ai\to j}R_{Ai\to j} \tag{6}$$

式中，Ω 为路径中可能经过节点的集合空间，Ψ 为发送节点对应的所有接收节点的集合空间。

博弈的结果要求发送者的期望 E_S 尽可能小，而窃听者要求其期望 E_A 尽可能大。所以使用混合博弈策略，用最小最大函数定义期望 $E_{S,A}$：

$$E_{S,A}=\min_{l_S\in S_\ell}\max_{l_A\in A_\ell}E^*(T) \tag{7}$$

式中，l_S 和 l_A 是路径集合空间 S_ℓ 和 A_ℓ 中的元素，$E^*(T)$ 为混合期望函数。

对路径 l_S 和 l_A 选择达到网络的最优路径，$E^*(T)$ 是 S_ℓ 和 A_ℓ 的函数。

$$E^*(T)=E_S+E_A \tag{8}$$

$$l_S=f_1(P_S,P_A),l_A=f_2(P_S,P_A) \tag{9}$$

路径 l_S 和 l_A 都是概率 P_S 和 P_A 的函数，通过上述策略，找出纳什均衡点处的最优路径对 (l_S,l_A)。

定理 1　当状态和行动的数量有限时，随机博弈中存在马尔可夫完美均衡[14]。

由于现存网络节点和所采取动作的有限性，因此模型中一定存在纳什均衡点 (l_S^*,l_A^*)。

5　仿真结果

在 MGBR 模型中，可以根据跳数、能量等不同的参数进行概率调整。本文中只考虑跳数对概率的影响。采用 PRISM 工具进行仿真实验。如图 6 所示，假设存在 $N\times N$ 个均匀分布的节点网络，其中 S 为源节点，E 为目的节点。数据从 S 向 E 传送，发送过程中窃听者进行窃听。

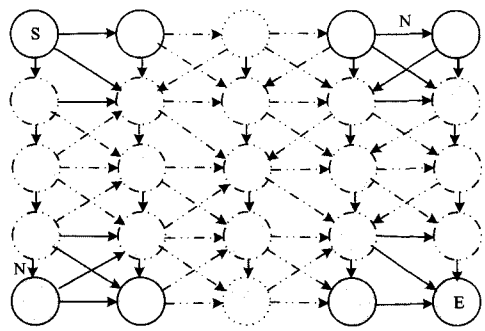

图 6　节点均匀分布图

其中发送概率根据式(1)、式(2)计算，而窃听概率通过式(3)计算。采用混合策略，通过式(4)－式(7)计算出混合策略的收益，根据收益的最终结果确定纳什均衡点概率。

仿真结果：

1)纳什均衡点存在性

为验证 MGBR 模型中纳什均衡点的存在，设节点个数 $N=10$，惩罚次数 $t=0,1,\cdots,10$。由于 t 的不同，数据被窃听的概率将随 t 的不同而变化，如图 7 所示。数据被窃听的概率开始随 t 的增大而减少，然后随 t 的增大而增大，当 $t=5$ 时为最小窃听概率，即纳什均衡点。

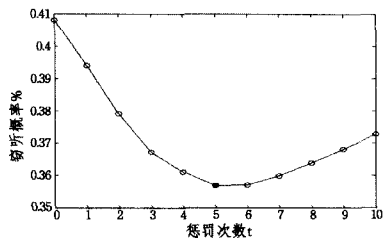

图 7　被窃听概率随惩罚次数 t 的变化图

（下转第 47 页）

[3] 任传伦. 分布环境下身份认证和授权管理的研究[D]. 北京:北京邮电大学,2007

[4] Beth T, Borcherding M, Klein B. Valuation of trust in open systems[C]// Gollmann D, ed. ESORICS'94, Lecture Notes in Computer Science. vol. 875. Berlin: Sringer-Verlag, 1994: 3-18

[5] Maurer U. Modelling a Public-Key Infrastructure Proc[C]// Bertino E, ed. 1996 European Symposium on Research in Computer Security(ESORICS'96). Lecture Notes in Computer Science. vol. 1146, Berlin: Springer-Verlag, 1996: 325-350

[6] Zhang Ming-de, Zheng Xue-feng, Yang Wen-sheng, et al. Research on Model of Trust Degrees for PKI[C]// The Fifth International Conference on Information Assurance and Security(IAS 2009). Volumes II. Xi'an, China, 2009: 647-650

[7] 汪伦伟,廖湘科,王怀民. 认证可信度理论研究[J]. 计算机研究与发展,2005,42(3):501-506

[8] Yahalom R, Klein B, Beth T. Trust Relationships in Secure Systems-A Distributed Authentication Perspective[C]// Proc. IEEE Symp on Research in Security and Privacy. 1993: 150-164

[9] Dierks T, Rescorla E. The Transport Layer Security(TLS) Protocol Version 1.1[S]. IETF, RFC 4346. April 2006

(上接第 36 页)

初始条件下所有发送(或转发)概率和窃听概率都是相等的,在相等情况下被窃听的概率不是最小,随着 t 的增大,被窃听的概率因发送概率和窃听概率的改变而变小。若惩罚次数 t 继续增大,随机路径趋向于单一路径,使被窃听的概率增大。

2)MGBR 策略前后窃听概率变化趋势及比较

通过 1)验证了纳什均衡点的存在,在纳什均衡条件下进行本次试验。通过该实验给出被窃听概率随节点的变化趋势,并与基于最小跳数算法的路由协议[15]下被窃听的概率进行比较。给出了节点 $N=4,5,6,7,8,9,10$ 时,被窃听的概率的变化趋势,如图 8 所示。

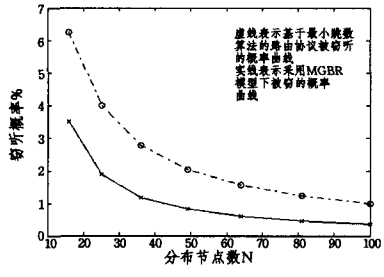

图 8 两种模型下被窃听概率随不同节点变化图

图中实线为 MGBR 策略下被窃听的概率,虚线表示基于最小跳数算法的路由协议下被窃听的概率。两种情况下曲线变化趋势都表明随着节点的增加,信息被窃听的概率减少,并且变化趋势逐渐趋于平缓。基于最小跳数算法的路由协议,由于没有采用概率传输,其节点被窃听的概率明显比 MGBR 策略下被窃听的概率高。采用 MGBR 策略可以有效降低信息被窃听的概率,提高网络的安全性。

结束语 本文针对 WSN 的路由寻址问题,给出了 MGBR 模型。定义了博弈双方,采用混合策略,通过概率转化进行模型的状态转移。模型针对网络中的窃听问题,给出了最优策略,使用 PRISM 工具进行仿真实验,得出了最优策略下的纳什均衡点,通过比较给出 MGBR 模型下信息被窃听的概率变化曲线。在传统路由中,窃听者具有记忆功能,在窃听数据之后,若发现该路径上的信息具有窃听价值,将记录该路径,并进行实时窃听,这给信息的保密带来威胁。在本文给出的 MGBR 模型中,路径的选择具有随机性,降低了路径被连续窃听的概率,提高了信息传输的安全性。

参 考 文 献

[1] Heinzelman W R, Chandrakasan A, Balakrish-nan H. Energy efficient communication protocol for wireless micro sensor networks[C]// Proc of the 33rd Hawaii International Conference on System Sciences. Maui, 2000: 3005-3014

[2] Sohrabi K, Gao J, Ailawad- hi V, et al. Protocols for self-organization of a wireless sensor network[J]. IEEE Personal Communications, 2000, 7(5): 16-27

[3] De S, Qiao C M, Wu H Y. Meshed multipath routing: An efficient strategy in sensor networks[J]. Computer Networks(Special Issue on Wireless Sensor Networks), 2003, 43(4): 482-497

[4] Estrin D, Govindan R, Heidemann J, et al. Next century challenges: Scalable coordinate in sensor network[C]// Proc of the 5th AC-M/IEEE International Conference on Mobile Computing and Networking. Seattle, 1999: 263-270

[5] Manjeshwar A, Agrawal D P. TEEN: A routing protocol for enhanced efficiency in Wireless Sensor Networks[C]// Proc of the 15th Parallel and Distributed Processing Symposium. San Francisco, 2001: 2009-2015

[6] 徐许亮,董荣胜,刘亮龙,等. 无线自组网中基于定价机制的节点协作性研究[J]. 系统仿真学报,2009,21(18):5914-5918

[7] 徐许亮,董荣胜,刘亮龙. 无线自组网中节点协作的纳什均衡研究[J]. 计算机工程,2010,36(4):107-109

[8] 曾加,慕春棣. 基于不完全信息博弈的传感器网络能量平衡路由[J]. 自动化学报,2008,34(3):317-322

[9] 汪洋,林闯,等. 基于非合作博弈的无线网络路由机制研究[J]. 计算机学报,2009,32(1):54-68

[10] Qiu Li-li, Yang Y R, Zhang Yin, et al. On Selfish Routing in Internet-Like Environments[C]// Proc. ACM SIGCOMM '03. 2003: 151-162

[11] La R, Anantharam V. Optimal Routing Control: Repeated Game Approach[J]. IEEE Trans. Automatic Control, 2002, 47: 437-450

[12] Kannan R, Sarangi S, Iyengar S S. Sensor-Centric Energy-Constrained Reliable Query Routing for Wireless Sensor Networks [J]. J. Parallel and Distributed Computing, 2004, 64: 839-852

[13] Bohacek S, Hespanha J P, Junsoo L, et al. Game theoretic stochastic routing for fault tolerance and security in computer networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2007, 9: 1227-1240

[14] Fudenbreg D, Tirole J. Game Theory[M]. 黄涛,郭凯,龚鹏,等译. 北京:人民大学出版社,2006

[15] 张喆. 基于最小跳数的无线传感器网络改进路由算法设计[D]. 南京:南京理工大学,2008(10)