doi:10.3969/j.issn.1000-436x.2013.z1.032

车载自组网节点轨迹隐私攻防博弈模型

杨卫东[1,2]，何云华[2,3]，孙利民[2,3]

(1. 河南工业大学 信息科学与工程学院，河南 郑州 450001；2. 中国科学院 信息工程研究所 信息安全国家重点实验室，北京 100093；
3. 西安电子科技大学 计算机学院，陕西 西安 710071)

摘 要：针对主动攻击所发布车辆轨迹隐私的场景，利用信息熵量化攻击者和防御者的能力，采用博弈论对车辆轨迹隐私攻击和防御进行建模，并给出攻击和防御策略，分析了攻防双方之间的博弈过程。通过对真实轨迹数据分析，得出完全信息博弈下的纳什均衡点和相应攻击策略下的最优防御策略。

关键词：车载自组织网络；轨迹；隐私保护；博弈论

中图分类号：TP393.08 **文献标识码**：B **文章编号**：1000-436X(2013)Z1-0240-06

Attack-defense game model of node traces privacy preserving for vehicle ad hoc networks

YANG Wei-dong[1,2], HE Yun-hua[2,3], SUN Li-min[2,3]

(1. College of Information Science and Engineering, Henan University of Technology, Zhengzhou 450001, China;
2. SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China;
3. School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

Abstract: The vulnerability of published vehicle traces is a focus issue for vehicle ad hoc network. Aiming at the privacy of published traces with a game-theoretic model under the scene of the active attacks and defense actions were modeled, and the attack and defense games were analyzed. Also ability of an adversary and the goal that a defender wants to achieve by the information entropy were quantified. By the analysis of true traces, the Nash equilibrium point under the game of complete information and an optimal defense strategy providing the user with the best privacy level for each attack strategy were presented.

Key words: vehicular ad-hoc networks; trace; privacy preserving; game theory

1 引言

车载自组织网络（VANET, vehicle ad hoc networks）是未来智能交通系统的关键技术，也是目前国际上网络通信领域的研究热点之一。VANET 是一个由车载节点、路边基站和后端服务中心（器）组成的三层网络架构，它包含 2 种新的通信模式：车–车通信（V2V）和车–路通信（V2I）。VANET 的主要应用包括辅助安全驾驶、交通管理和车载娱乐(infotainment)等应用。近年来，VANET 已引起国内外政府、学术界和产业界的广泛关注和深入研究。

如何使得车辆用户能主动上传其车辆位置信息，为道路交通实时状况发布提供支撑，为车辆驾驶员提供实时路况信息，为探索新的商业服务模式提供基础数据，具有重要的应用价值。然而，车辆移动轨迹信息与车辆、驾驶员具有很强的关联性，攻击者可能会利用发布的数据，结合新闻、社交网络和博客等间接信息，还原目标车辆的行驶轨迹，获取和泄露车辆所有者的身份和社会活动，泄露信息提供者的隐私。因此，车辆轨迹隐私保护问题成为当前 VANET 研究领域中的一个热点。

Hoh 等[1,2]指出 *k*-anonymity 算法能够满足交通管

收稿日期：2013-07-10
基金项目：国家自然科学基金资助项目（61202099，61073180）；中国博士后科学基金资助项目（2013M530706）
Foundation Items: The National Natural Science Foundation of China (61202099, 61073180), The China Postdoctoral Science Foundation Funded Project (2013M530706)

理对位置准确性的要求，但不能保证车辆稀疏区域用户的隐私保护。Jin 等[3]提出了时间不可关联性的概念，即攻击者无法将用户的信息关联在一起。考虑位置信息时空关联性因素，Nergiz 等[4]重新定义了 *k*-anonymity 的概念，并首次提出了基于归纳的轨迹匿名化方法。Mehmet 等[5]采用 *k*-匿名实现轨迹匿名，能够保证每条轨迹至少与其他 *k*–1 个轨迹不可区分，同时，他们设计随机重构算法对发布的匿名轨迹进行处理。Lu 等[6]提出一种社会热点匿名改变机制，来保证 VANET 中的车辆位置隐私。Chris 等[7]指出攻击者可以利用节点的少量位置快照，标识出轨迹集中某一节点的轨迹。他们量化了节点的隐私泄露，由节点移动性、攻击者的推断策略、噪声来计算，并证实攻击者利用很少的信息就可以推断出节点真实的 ID。

尽管许多学者研究了车辆轨迹隐私保护问题，但目前缺少相应的方法和模型去分析和量化轨迹隐私泄露问题。当前，博弈论正被用来研究无线网络的安全与隐私问题。Raya 等人[8]基于博弈论研究了间歇网络中恶意节点撤销问题，即利用参与者合作来决定是否撤销潜在的恶意参与者。Reidt 等人[9]采用博弈论方法设计了一种 ad hoc 网络中的分布式健壮动态撤销机制，激励诚实节点对恶意节点进行撤销。Alpcan 等人[10]利用零和博弈、模糊博弈和虚拟游戏分析了车载自组网中攻击者和防御者之间交互过程。

本文针对文献[7]中提出的主动攻击场景，首先利用信息熵来量化攻击者的攻击能力和防御者的防御能力，进一步采用博弈论对攻防过程进行建模，给出相应的攻击策略和防御策略，分析了攻击者与防御者之间的博弈过程，提出了最优防御策略。

2　场景及定义

2.1　场景

攻击者对所发布的车辆轨迹隐私的攻击，目的是从匿名轨迹集中确定所攻击车辆的完整历史轨迹。

假定攻击者可以收集关于一个或多个车辆轨迹的边信息（side information），每一份边信息给出了某一时刻一个参与者的位置信息，该信息也可能是不准确的。在主动攻击场景中，攻击者试图通过与参与者相遇的方式获得边信息。攻击者知道完整的路径集，而且知道实时、渐进的路径集，例如，随时间的推移，攻击者不仅知道以前的路径集，还知道实时获取的路径集。这里攻击者的目标是，仅可能确定更多节点的真实路径。

在文献[7]中，主动攻击主要包括以下 2 种情形：（B1）攻击者不动，此时可获得边信息最少；（B2）节点提前设定好移动策略，从而使得可获得边信息最多，但与其他节点一样，会受到道路拓扑的限制和速度限制。

本文不考虑攻击者采用受害节点的移动策略，也就是说，当遇到一个节点后，攻击者不会尝试跟踪该节点，这是因为在该场景下攻击者的目标是尽可能确定更多节点的真实路径。

2.2　定义

在建立攻防博弈模型之前，首先利用信息熵定义目标节点（被攻击节点）轨迹隐私泄露程度，进而定义攻击者的攻击能力和防御者的防御能力。

定义 1　设 L_i 为节点 i 的轨迹，所有节点的轨迹集 $Trace=\{L_i|\ i$ 为节点$\}$，并设 L_i 为目标节点 T 的轨迹的概率为 $p_i=\Pr(L_T=L_i)$，$\forall L_i\in Trace$，其中，$\sum_{i=1}^{|Trace|}p_i=1$，那么可将目标节点 T 的轨迹集分布熵定义为

$$H(L_T)\sum_{i=1}^{|Trace|}p_i\mathrm{lb}p_i \tag{1}$$

分布熵 $H(L_T)$越大，目标节点 T 的轨迹不确定性越高；分布熵 $H(L_T)$最小，目标节点 T 的轨迹不确定性越低，当 $H(P)=0$ 时，就可以唯一确定目标节点的轨迹。

假设 R 为受害节点的边信息，R 是一个映射：$R:\{t_k\}\to\Theta$，其中，t_k 为边信息所揭示的受害节点的时间实例（time instant），Θ 为所有单元格（cell）位置 ID 集合，于是 $R(t_k)$表示攻击者在时刻 t_k 获得受害节点所在单元格的位置 ID。那么攻击者获取某个节点轨迹的能力可表示为条件熵的形式。

定义 2　攻击者获取目标节点 T 轨迹的能力可表示为条件熵：

$$H(L_T\mid R)=-\sum_{i=1}^{|Trace|}\sum_k\Pr(L_i,R(t_k))\mathrm{lb}\Pr(L_i\mid R(t_k)) \tag{2}$$

其中，$\Pr(L_i|R(t_k))$表示攻击者在已知 $R(t_k)$的情况下确定目标节点 T 的路径为 L_i 的概率，$\Pr(L_i, R(t_k))$为攻击者已知边信息 $R(t_k)$且目标节点 T 的路径为 L_i 的概率，它们分别为条件概率和联合概率。

由于 $H(L_T\mid R)=\sum_k\Pr(R(t_k))H(L_i\mid R(t_k))$，因此攻击者的能力与获取边信息的准确性 $\Pr(R(t_k))$，以及边信息下的条件熵 $\mathrm{H}(L_T|R(t_k))$相关。$\Pr(R(t_k))$取固定时，$\mathrm{H}(L_T|R(t_k))$越大，$\mathrm{H}(L_T|R)$也越大，则攻击者

的能力越弱；$H(L_T|R(t_k))$越小，$H(L_T|R)$也越小，则攻击者的能力越强，当 $H(L_T|R)$为 0 时，攻击者可以唯一目标节点的轨迹。

防御者实现轨迹隐私保护的能力用匿名集来度量，本文采用 *k*-匿名熵度量（如定义 3 所示）。

定义 3 设防御者 S 需要提供至少大小为 k 的匿名集，该 *k*-匿名集熵可表示为

$$H(S)=-\sum_k (1/k)\mathrm{lb}(1/k)=\mathrm{lb}k \tag{3}$$

那么防御者的轨迹隐私保护机制，应满足

$$H(L_T \mid \Omega) \geqslant H(S) \tag{4}$$

其中，Ω 为防御者假设攻击者已掌握的边信息，$H(L_T \mid \Omega)$ 为防御者在 Ω 下被标识出轨迹的不确定度。

3 攻防博弈模型

3.1 博弈模型

针对攻击者的不同攻击策略，建立博弈模型，以便获得对应攻击策略下的最优防御策略。攻防博弈 G 可定义为三元组(P,S,U)，其中，P 是参与者集合，S 是策略集，U 是收益函数集。

参与者：参与者集合 $P=\{P_i|0<i\leqslant I\}$，这里假定 $I=2$，即分别对应攻击者和防御者，其中攻击者有 2 种类型：全局的被动攻击者（GPA, global passive adversary）和局部主动攻击者（LAA, local active adversary）。

策略：博弈中的策略集 $S=\{S_i|0<i\leqslant I\}$，其中，S_1 为攻击者策略集，S_2 为防御者策略集，将在 5.3 节和 5.4 节详细介绍。

收益函数：当防御者知道攻击者所掌握的边信息时，建立完全信息博弈，此时攻击者的收益为 $u_1(s_1,s_2)=H(L_T \mid R)-\gamma_1$，防御者的收益为 $u_2(s_1,s_2)=H(L_T \mid \Omega)-\gamma_2$，$\gamma_1,\gamma_2$ 分别表示攻击和防御代价。这里为了最大化攻击者的能力，将 γ_1 设为 0；γ_2 包括防御措施的代价，以及它对数据真实性造成的影响。

3.2 攻防策略

3.2.1 攻击策略介绍

在主动攻击场景中，攻击者直接观察参与者，根据观察到的信息与发布轨迹之间的对应关系，实时揭示参与者轨迹。由于攻击者直接观察的信息不存在噪声，所以不需要任何推断操作。攻击算法可描述如图 1 所示。

```
Input: {Li|i=1,2,…, N}
Output: Identified traces
Begin:
For(m=0; m<number_of_trace; m++)
{  /*initially all traces are possible candidates to each victim*/
   Candidate_setm={Li|i=1,2,…, N}
}
While(sampling_time not ended)
{    For each node i met at sampling_time and j∈Candidate_seti
If(met node i at location r at sampling_time and Lj(sampling_time)!=r)
{   remove trace j from Candidate_seti
    If(|Candidate_seti|=1)
        Cascade(Candidate_set,m)
}
Evolve sampling_time.
}
Cascade(Candidate_set,i)
{   Lj∈Candidate_seti is the identified trace
for(m=0; m<number_of_trace; m++)
If(Lj∈Candidate_seti in Candidate_setm and m≠i)
{   remove Lj from Candidate_setm
    If(|Candidate_setm|=1)
    Cascade(Candidate_set,m)
}
}
End
```

图 1 主动攻击算法

算法以不断地发布轨迹作为输入。初始时，假定对于每个参与者，所有的轨迹都是候选轨迹。如果一条轨迹出现的时间、位置与攻击者遇到某个参与者的时间、位置相同，则称这条轨迹是该参与者的候选轨迹。随着时间推移，攻击者从受害节点集合中剔除与观察信息不一致的候选轨迹。当受害节点轨迹被确定时，调用 Cascade 函数，该函数将这条路径从其他受害节点的候选轨迹中移除。注意：攻击者多次与一个参与者相遇也可能不能确定该参与者，但是随着其他候选轨迹被确定移除，剩余的最后一条候选轨迹就是该参与者的轨迹，即图 1 中递归“级联”函数所描述的过程。因此，当攻击者试图确定多个参与者轨迹时相对更高效。

3.2.2 防御策略

通常，隐私保护即防御策略有匿名技术和隐藏技术。设 *Trace* 为节点的轨迹集，$\{s_1, s_2,\cdots, s_k,\cdots\}$ 为抽样时间序列，防御策略可表述如下。

策略 D1：向 *Trace* 添加 m 个节点的轨迹集组成新的轨迹集 *Trace*′，使得 *Trace*′ ⊃ *Trace*，且满足 $|Trace'| = |Trace| + m$。

策略 D2：删除序列$\{s_1, s_2,\cdots, s_k,\cdots\}$中的 n 个抽

样时间点，组成新的抽样时间序列 $\{s'_1, s'_2, \cdots, s'_k, \cdots\}$，使得 $\{s_1, s_2, \cdots, s_k, \cdots\} \supset \{s'_1, s'_2, \cdots, s'_k, \cdots\}$。

4　实验分析

本文实验数据采用美国旧金山 536 辆出租车 23 天内的行驶轨迹，原始数据集由一系列时间有序的车辆位置和状态数据组成。

为了降低实验分析难度，对于策略 D1，防御代价 γ=0 满足以下关系式

$$\gamma = \alpha \frac{m}{|Trace|} \tag{5}$$

其中，α 为比例参数，|*Trace*|为节点轨迹总数，*m* 为添加轨迹的条数。例如添加 *m*=|Trace|/2 条轨迹，那么其防御代价为 $\gamma=\alpha/2$。

对于策略 D2，防御代价 γ 满足以下关系式

$$\gamma = \beta \frac{n}{N} \tag{6}$$

其中，β 为比例参数，N 为抽样时间点的总数，n 为删除抽样点的个数。例如删除 $n=N/2$ 个抽样时间点，那么其防御代价为 $\gamma=\beta/2$。防御者采用 D1、D2 这 2 种防御策略，令 $\gamma^4=\beta/2, \gamma^5=3\beta/4, \gamma^6=7\beta/8$ $\gamma^1=a/8, \gamma^2=a/4, \gamma^3=a/2$，并令 m=0, |*Trace*|/8, |*Trace*|/4, |*Trace*|/2，n=0, *N*/2, 3*N*/4, 7*N*/8。

针对 B1、B2 的完全信息博弈的策略式如图 2~图 5 所示，其中，攻击策略分别执行了 60 min、100 min、400 min、600 min。当 γ=0 时，执行 60 min、100 min、400 min 后的纳什均衡为(B2, m=|*Trace*|/2)、(B2, n=7*N*/8)，执行 600 min 后的纳什均衡为(B1, m=|*Trace*|/2)、(B1, n=7*N*/8)。

考虑防御代价时，不同 α，β 取值下的最优防御

	m=0	$m=\frac{\|Trace\|}{8}$	$m=\frac{\|Trace\|}{4}$	$m=\frac{\|Trace\|}{2}$
B1	2.27,2.27	2.43,2.43−γ^1	2.59,2.59−γ^2	2.85,2.85−γ^3
B2	1.37,1.37	1.54,1.54−γ^1	1.69,1.69−γ^2	1.96,1.96−γ^3

(a) 防御者采取D1策略

	n=0	n=N/2	n=3N/4	n=7N/8
B1	2.27,2.27	3.27,3.27−γ^4	4.26,4.26−γ^5	5.28,5.28−γ^6
B2	1.37,1.37	2.27,2.27−γ^4	3.28,3.28−γ^5	4.27,4.27−γ^6

(b) 防御者采取D2策略

图2　攻击策略执行60 min时的完全信息博弈

	m=0	$m=\frac{\|Trace\|}{8}$	$m=\frac{\|Trace\|}{4}$	$m=\frac{\|Trace\|}{2}$
B1	1.68,1.68	1.85,1.85−γ^1	2.01,2.01−γ^2	2.27,2.27−γ^3
B2	1.27,1.27	1.44,1.44−γ^1	1.59,1.59−γ^2	1.85,1.85−γ^3

(a) 防御者采取D1策略

	n=0	n=N/2	n=3N/4	n=7N/8
B1	1.68,1.68	2.68,2.68−γ^4	3.68,3.68−γ^5	4.68,4.68−γ^6
B2	1.27,1.27	2.26,2.26−γ^4	3.27,3.27−γ^5	4.27,4.27−γ^6

(b) 防御者采取D2策略

图3　攻击策略执行100 min时的完全信息博弈

	m=0	$m=\frac{\|Trace\|}{8}$	$m=\frac{\|Trace\|}{4}$	$m=\frac{\|Trace\|}{2}$
B1	0.37,0.37	0.54,0.54−γ^1	0.69,0.69−γ^2	0.96,0.96−γ^3
B2	0.35,0.35	0.52,0.52−γ^1	0.67,0.67−γ^2	0.94,0.94−γ^3

(a) 防御者采取D1策略

	n=0	n=N/2	n=3N/4	n=7N/8
B1	0.37,0.37	1.37,1.37−γ^4	2.38,2.38−γ^5	3.37,3.37−γ^6
B2	0.35,0.35	1.34,1.34−γ^4	2.35,2.35−γ^5	3.35,3.35−γ^6

(b) 防御者采取D2策略

图4　攻击策略执行400 min时的完全信息博弈

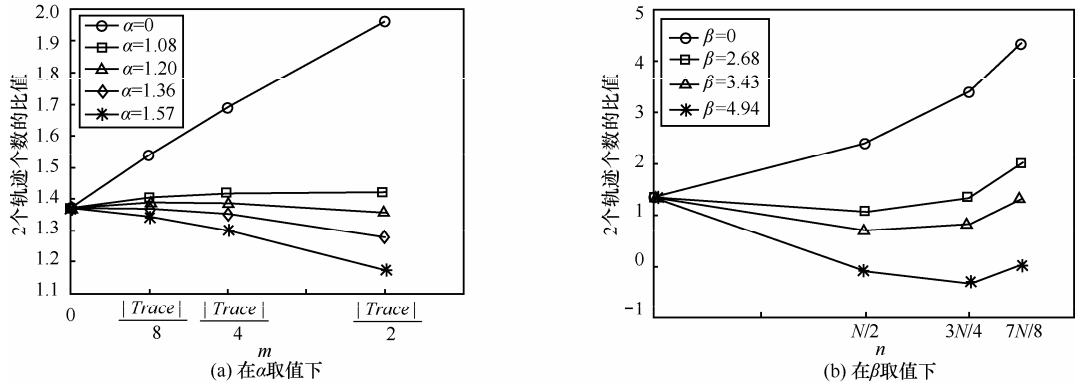
	m=0	$m=\frac{\|Trace\|}{8}$	$m=\frac{\|Trace\|}{4}$	$m=\frac{\|Trace\|}{2}$
B1	0.14,0.14	0.31,0.31−γ^1	0.46,0.46−γ^2	0.73,0.73−γ^3
B2	0.19,0.19	0.36,0.36−γ^1	0.51,0.51−γ^2	0.77,0.77−γ^3

(a) 防御者采取D1策略

	n=0	n=N/2	n=3N/4	n=7N/8
B1	0.14,0.14	0.14,0.14−γ^4	2.15,2.15−γ^5	3.14,3.14−γ^6
B2	0.19,0.19	0.19,0.19−γ^4	2.18,2.18−γ^5	3.19,3.19−γ^6

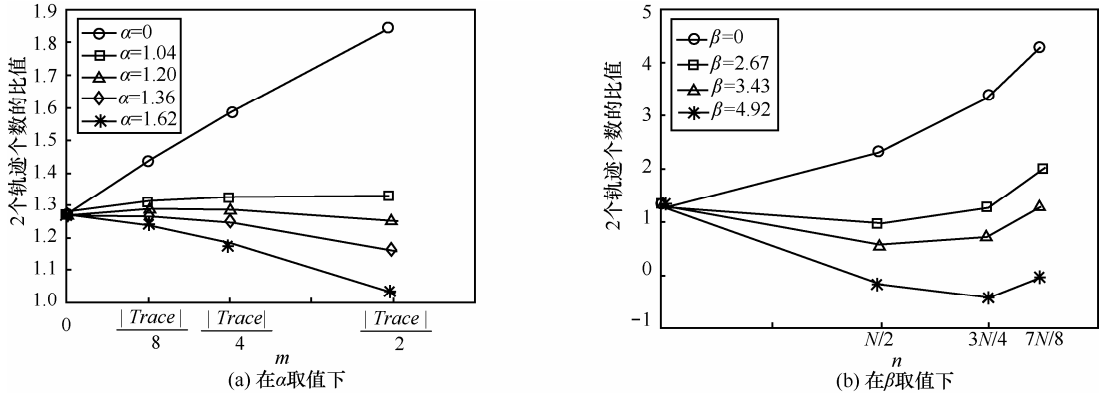
(b) 防御者采取D2策略

图5　攻击策略执行600 min时的完全信息博弈



(a) 在α取值下　　(b) 在β取值下

图 6　攻击策略执行 60 min 时，不同 α,β 取值下的最优防御策略



(a) 在α取值下　　(b) 在β取值下

图 7　攻击策略执行 100 min 时，不同 α,β 取值下的最优防御策略

策略如图 6 和图 7 所示，每条线的最大值点对应于最优防御策略。从整体来看，当$0\leqslant\alpha\leqslant1.04$时，最优策略为 m=|*Trace*|/2，当$1.08\leqslant\alpha\leqslant1.20$时，最优策略为 m=|*Trace*|/4，当$1.20\leqslant\alpha\leqslant1.36$时，最优策略为 m=|*Trace*|/8，当$\alpha\geqslant1.36$时，最优策略为 m=0；当$0\leqslant\beta\leqslant3.43$时，最优策略为 n=7*N*/8，当$\beta\geqslant3.43$时，最优策略为 n=0。

5　结束语

本文采用博弈论方法研究了 VANET 中轨迹泄露问题。首先采用条件熵来量化攻击和防御能力，实现了攻击能力与防御效果的可比性。在攻防博弈中，从主动攻击建立攻击者行为模型，从添加虚假轨迹和删除抽样时间点来建模网络防御行为。最后，针对不同的攻击策略，利用完全信息博弈进行分析，得到了相应攻击策略下的最优防御策略。下一步，将采用更多的轨迹集来进行验证，并给出可行的轨迹隐私保护策略。

参考文献：

[1] HOH B, GRUTESER M, XIONG H, *et al*. Preserving privacyin GPS traces viaun certainty-aware path cloaking[A]. CCS'07: Proceedings of the 14th ACM Conference on Computer and communications Security[C]. New York, NY, USA, 2007.161-171.

[2] HOH B, GRUTESER M, XIONG H, *et al*. Achieving guaranteed anonymity in GPS traces via uncertainty-aware path cloaking[J]. IEEE Transactions on Mobile Computing. 2010, 9(8):1089-1107.

[3] JIN W, LEFEVRE K, PATEL J M. An online framework for publishing privacy-sensitive location traces[A]. MobiDE'10: Proceedings of the Ninth ACM International Workshop on Data Engineering for Wireless and Mobile Access[C]. New York, NY, USA, 2010.1-8.

[4] NERGIZ M E, ATZORI M, SAYGN Y, *et al*. Towards trajectory anonymization: a generalization-based approach[J]. Trans Data Privacy, 2009, 2(1):47-75.

[5] NERGIZ M, ATZORI M, SAYGIN Y, *et al*. Towards trajectory anonymization: a generalization-based approach[J]. Journal Transactions on Data Privacy, 2009, 2(1):47-75.

[6] LU R X, LIN X S, LUAN T H, *et al*. Pseudonym changing at social spots: an effective strategy for location privacy in VANETs[J]. IEEE

Transactions on Vehicular Technology. 2012, 61(1):86-96.

[7] MA C Y T, YAU D K Y, YIP N K, Privacy vulnerability of published anonymous mobility traces[A]. Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking (Mobicom'10)[C]. New York, USA, 2010. 185-196.

[8] RAYA M, MANSHAEI M H, FELEGYHAZI M, *et al*. Revocation Games in Ephemeral Networks[A]. ACM Conference on Computer and Communications Security (CCS)[C]. New York, NY, USA, 2008. 199-210.

[9] REIDT S, SRIVATSA M, *et al*. The fable of the bees: incentivizing robust revocation decision making in ad hoc networks[A]. ACM Conference on Computer and Communications Security (CCS)[C]. New York, NY, USA, 2009. 291-302.

[10] ALPCAN T, BUCHEGGER S, Security games for vehicular networks[J]. IEEE Transactions on Mobile Computing, 2011, 10(2): 280-290.

作者简介：

杨卫东（1977-），男，内蒙古集宁人，博士，河南工业大学副教授，主要研究方向为车联网、信息安全等。

何云华（1987-），男，湖北荆门人，中国科学院信息工程研究所博士生，主要研究方向为车联网、信息安全等。

孙利民（1966-），男，河南淮阳人，中国科学院信息工程研究所研究员，主要研究方向为无线传感器网络、信息安全等。

（上接第 239 页）

GUO W F. Research on the Secure Crossing-domains Transmission Schema for the EPC Networks [D]. Zhengzhou: PLA Information Engineering University, 2011.

[8] 郭卫锋, 李景峰, 张来顺. EPC 网络中一种可证明安全的跨域认证协议[J]. 小型微型计算机系统, 2013, 34(5):983-986.
GUO W F,LI J F, ZHANG L S. A provable secure crossing-domains authentication protocol for the EPC networks[J]. Journal of Chinese Computer Systems, 2013, 34(5):983-986.

[9] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报, 2006, 29(8):1271-1281.
PENG H X. An Identity-based authentication model for multi-domain[J]. Chinese Journal of Computers, 2006, 29(8):1271-1281.

[10] 朱辉, 李晖, 杨加喜等. 一种可证明安全的通用多信任域认证协议[J]. 武汉大学学报（信息科学版）, 2008, 33(10):1051-1054.
ZHU H, LI Y, YANG J X, *et al*. A universal provable security authentication protocol for multi-domain[J]. Geomatics and Information Science of Wuhan University, 2008, 33(10):1051-1054.

作者简介：

李景峰（1977-），男，江苏南京人，解放军信息工程大学副教授、硕士生导师，主要研究方向为信息系统安全技术、无线移动通信网网络等。

潘恒（1977-），女，河南新乡人，中原工学院计算机学院副教授、硕士生导师，主要研究方向为信息系统安全测评等。

郭卫锋（1987-），男，河南周口人，解放军信息工程大学硕士生，主要研究方向为物联网安全基础设施。