doi:10.11959/j.issn.1000-436x.2017055

VANET 中位置相关的轻量级 Sybil 攻击检测方法

辛燕[1]，冯霞[2]，李婷婷[1]
（1. 江苏大学计算机科学与通信工程学院，江苏 镇江 212013；
2. 安徽大学信息保障技术协同创新中心，安徽 合肥 230601）

摘 要：在车联网中，同时使用多个虚假身份的 Sybil 攻击，在网络中散布虚假消息，都易造成资源的不公平使用和网络混乱。针对这一问题，提出快速识别车辆虚假位置的事件驱动型轻量级算法，当车辆出现在另一车辆的安全区域内，启动快速识别两车辆是否重叠的几何交叉模型（GCR, geometrical cross-recognition）算法，检测声称虚假位置的错误行为；同时，根据证实车辆收集的邻居范围内的局部车辆，建立位置偏差矩阵（PDM, position deviation matrix），进一步识别交叉车辆中的 Sybil 节点。性能分析和仿真实验表明，安全区域驱动下的轻量级算法识别速度快，检测率高，在车辆定位误差较低时性能更好；安全区域的引入也均衡了车辆密度过大时造成的通信负载影响，与同类算法相比，通信处理时延较低。

关键词：Sybil 攻击；几何交叉模型算法；位置偏差矩阵；轻量级算法
中图分类号：TP393 **文献标识码**：A

Position related lightweight Sybil detection approach in VANET

XIN Yan[1], FENG Xia[2], LI Ting-ting[1]
(1. School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China;
2. Information Assurance Technology Collaborative Innovation Center, Anhui University, Hefei 230601, China)

Abstract: In VANET, the Sybil attack simultaneously using multiple forged identities can easily cause the injustice of resource usage and make networks in a mess by distributing false messages. To solve this problem, an event-driven lightweight algorithm was proposed, which could identify vehicles false position quickly. When one vehicle appeared inside another's safety zone, a geometrical cross-recognition algorithm to calculate the overlap between vehicles to detect false position claiming was presented. At the same time, according to the neighbors within the confirming vehicle's radio range, position deviation matrix was established further to identify the Sybil node of two overlap vehicles. The performance analysis and simulation results show that the lightweight algorithm driven by safety zone demonstrates fast identification and high detection rate, especially when GPS error is very low. The imported safety zone can also balance the communication load impacting by heavy vehicular density. And the communication processing delay is lower than other approaches.

Key words: Sybil attack, geometrical cross-recognition algorithm, position deviation matrix, lightweight algorithm

1 引言

车联网[1~3]（VANET, vehicular ad hoc network）是一种特殊的移动 ad hoc 网，将每一辆车作为一个信息源，利用无线通信手段，建立以车为节点，人、车、路间交互的信息系统。这种无中心的网络，车辆节点在缺少固定基础设施的情形下也能直接通信，构成 V2V(vehicle-to-vehicle)和 V2I(vehicle-to-infrastructure) 这 2 种通信模式[4]。无线通信以代表网络节点的唯一身份标识为基础，但 VANET 中变化频繁且分散开放的无线网络拓扑结构[5]，使节点身份易被盗用或易被伪造虚假身份，Douceur 等将

收稿日期：2016-10-11；修回日期：2017-01-16
基金项目：国家自然科学基金资助项目（No.61472001）；江苏省重点研发计划基金资助项目（No.BE2015136）
Foundation Items: The National Natural Science Foundation of China (No.61472001), The Key Research and Development Project of Jiangsu Province (No.BE2015136)

此称为 Sybil 攻击。恶意车辆在同一时刻或连续的时间段内声称有多个身份后，散布虚假消息或拒绝消息服务，进一步还可引发其他类型的攻击，对风险警告、防碰撞、辅助驾驶等安全相关的应用造成多种威胁。若不采取有效的预防措施，到 2030 年，由此引发的道路伤亡将成为人类第五大死亡原因[6]。

VANET 中的一类 Sybil 攻击是攻击者生成任意数目的虚假车辆，且同时使用所有的虚假身份，在网络中传播虚假消息，以引起网络混乱或企图拥有比单个节点更多的资源、信息和网络访问等。一些自私的驾驶者为独享道路制造交通拥堵的假象[7]是此类攻击的模式之一，如图 1 所示，车辆 N_m 为制造 Sybil 攻击的恶意节点，Ns_1、Ns_2 是 N_m 伪造的 Sybil 节点，当正常车辆 N_n 驶近时，它从接收到的消息判断前方发生了交通拥堵，从而绕道行驶，给车辆的正常出行带来了不便。

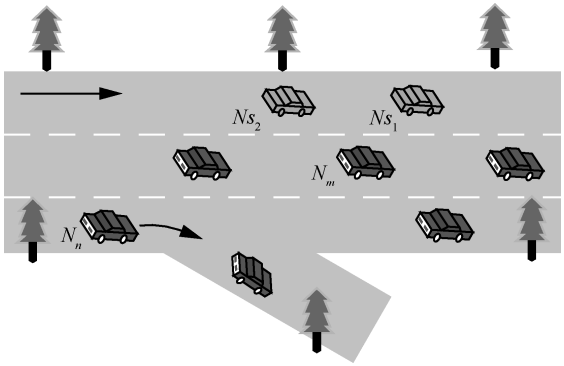

图 1　Sybil 攻击制造的虚假拥堵

在上述 Sybil 攻击中，恶意节点依赖伪造的不同位置信息，同时声称了多个身份，因同一时刻不同物理车辆应出现在不同的物理位置，故某时刻的位置与车辆身份之间存在一定关联，因此，对虚假身份的识别可转化为对车辆所处位置的真实性验证。

VANET 中通过验证位置信息检测 Sybil 攻击，多数是一种非认证的方法，避免了无线电资源检测方案受限于节点只有一个无线设备且一次只能在一个信道上收发数据的假设，减少了加密认证方案中对上层复杂的加密和密钥管理技术的依赖，已成为前景较为广阔的一种研究方案[13]。位置相关的 Sybil 攻击检测方案，包括车辆路径轨迹检测[8~10]、基于接收信号强度指示的检测[11~13]、基于协作的邻居车辆位置合理性检测[13~16]。在车辆路径轨迹检测方案[9]中，将车辆行驶过程中经过的路边单元（RSU, road side unit）记为车辆行驶轨迹的标记（RSU_1, RSU_2,…, RSU_n），因恶意车辆（发起 Sybil 攻击的车辆）和 Sybil 车辆（Sybil 攻击伪造的车辆）始终具有完全相同的运动路径，这与现实中任何 2 个车辆不会在一段时间内的相同时刻经过相同的 RSU，且一个车辆不可能同时出现在多个不同的 RSU 处的特征不符，故可识别出 Sybil 攻击，该方法对 RSU 依赖性较大，需要借助多个 RSU，无法抵御 RSU 被俘获的攻击。基于接收信号强度的检测方案，由无线电模块中的接收信号强度指示器（RSSI，received signal strength indication）估算信号发送者的距离，比较车辆节点自我声称的位置与 RSSI 估算位置以验证车辆位置的合理性，但 RSSI 的估算值往往受环境中多径、散射、障碍物、电磁干扰等不稳定因素的影响，具有较大的波动性，因此，估算位置信息的精确度有待提高，给检测结果造成了不良影响。基于邻居车辆位置合理性检测方案是指邻居节点协作地验证局部范围内车辆位置的合理性，文献[15]提出了一种利用节点间邻居信息的相似性检测 Sybil 攻击的方法，车辆节点间相互广播各自的信息，每个车辆得到自己的邻居节点集合之后，与单跳范围内的车辆交换邻居节点集合，观察在一段时间 t 内邻居节点集合的交集，如果交集不为空，即在时间 t 内所有车辆的邻居节点中有相同车辆，相同的车辆就被认为是 Sybil 车辆，一般当恶意车辆和 Sybil 车辆在局部区域中占较大比例时此类方法检测率降低。

针对同时性 Sybil 攻击——恶意车辆通过散播事先准备好的包含不同位置信息的 CAM (cooperative awareness message)来声称多个车辆的存在，伪造多个身份在网络中同时出现，但这些身份代表的车辆并不真实存在于某路段上的场景，本文提出一种不依赖特定外界设备，能快速识别车辆虚假位置的事件驱动型轻量级算法，以适应车联网环境安全实时性要求高的特点。

本文所提事件驱动型算法只有当车辆出现在另一车辆的安全区域内才会被触发。对安全区域内出现的车辆，根据同一时刻同一物理位置不可能有 2 个车辆同时出现的原理设计了快速识别 2 个车辆是否重叠的几何交叉模型算法，从而检测恶意行为的存在；同时由证实车辆（启动了快速检测算法的车辆）建立邻居范围内的局部车辆位置偏差矩阵，进一步识别交叉车辆的真伪。

2 网络攻击模型和假设

本文讨论利用多重身份来同时投放多个虚拟车辆的 Sybil 攻击。车联网中每个车辆被称为节点，攻击由某一恶意节点发起，在通信范围内的一跳邻居节点间周期性广播事先准备好的包含虚假位置、速度等信息的 CAM，该消息符合文献[17,18]中提出的基本运动合理性模型，被误认为是由道路上行驶的“真实”车辆发送，此类节点称为 Sybil 节点。恶意节点和 Sybil 节点本质上为同一车辆，因此这里假设相互之间无射频通信。

假设车联网中所有车辆节点具有基本的通信单元和 GPS 导航系统，能实时采集位置、速度、方向等自身交通信息。GPS 定位误差范围为 10~15 m，恶意节点伪造的虚假位置均在节点自身 GPS 定位误差之外，其真实位置在 GPS 测量误差范围之内。节点独立运行，采集的车辆实时交通信息以 CAM 格式在节点的一跳范围内周期性广播；CAM 参考文献[17]被定义成六元组形式 *CAMS*(*NID*, *MID*, *T_Stamp*, *Azimuth*, *Velocity*, *GPS*)，其中，*NID* 和 *MID* 分别为节点编号和消息编号，*T_Stamp* 为时间戳，*Azimuth*、*Velocity* 分别为车辆的方位和速度，*GPS* 数据中包含了车辆的位置信息。

车辆收集局部范围内的 CAM 消息，建立对应的邻居列表 *NebList*(*Nid*, *pos*, *vel*, *time_stamp*)，由邻居列表可得到节点的邻居观察 $Obs(Nid_1, Nid_2, \cdots, Nid_n)$。

在网络中，假设每个真实车辆都支持几何交叉模型快速检测算法，位置信息的证明无需 RSU 等特定外界设备的支持，且不涉及车辆隐私问题。

3 事件驱动的轻量级 Sybil 节点检测方案

真实车辆根据接收到的邻居 CAM 消息，判别某一车辆是否出现在另一车辆的安全车距内，若是，则启动几何交叉快速检测算法，故称为事件驱动型算法，同时要求邻居车辆报告邻居观察，由证实车辆建立邻居范围内的局部车辆位置偏差矩阵，进一步识别交叉车辆的真伪。上述检测过程无需借助特定的硬件或基础设施，几何交叉快速检测算法以及位置偏差矩阵的建立所需计算开销小，因此为轻量级检测方案。

3.1 安全车距确定

安全车距作为车辆的主要安全系数之一，在车辆防碰撞系统中常被使用[26,27]。本文借助安全车距概念，提出一种识别虚假车辆的事件驱动型算法，对出现在安全车距内即危险区域的车辆启动检测。

汽车安全行车距离受车辆行驶速度、驾驶员反应能力、路面状况、天气变化及车辆制动系统结构等多种因素的综合影响[24]，情况复杂，根据与安全车距 $dist_{SD}$ 相关的反应距离 $dist_{RD}$、制动距离 $dist_{BD}$ 和静止安全距离 $dist_{MD}$ 这 3 个重要组成部分，定义如式(1)所示的安全车距模型，假设车辆行驶速度为 v。

$$\begin{cases} dist_{SD} = dist_{RD} + dist_{BD} + dist_{MD} \\ dist_{RD} = vt_{rs} \\ dist_{BD} = \dfrac{v^2}{2gf} \end{cases} \tag{1}$$

其中，反应距离与驾驶员反应时间 t_{rs} 有关，对于普通驾驶员，反应时间为 0.3~1 s；制动距离受轮胎与路面摩擦系数为 f，g 为重力加速度，表 1 列出了摩擦系数和车速之间的关系；最小静止安全距离一般为 2~5 m。

表 1 摩擦系数与车速关系

车速/(km·h^{-1})	摩擦系数	车速/(km·h^{-1})	摩擦系数
30	0.40	80	0.34
40	0.38	90	0.33
50	0.37	100	0.32
60	0.36	110	0.31
70	0.35	120	0.30

图 2 显示了最小静止安全距离 $dist_{MD}$=3 m，反应时间分别取 0.2 s、0.4 s、0.6 s、0.8 s、1 s 时，车辆运行在不同速度下的安全车距。在同一反应时间下，安全车距随车速增长明显，而在同一速率下不同反应时间下安全车距的变化最大差异在 7 m 左右，因此，车速是影响安全车距的主要因素。

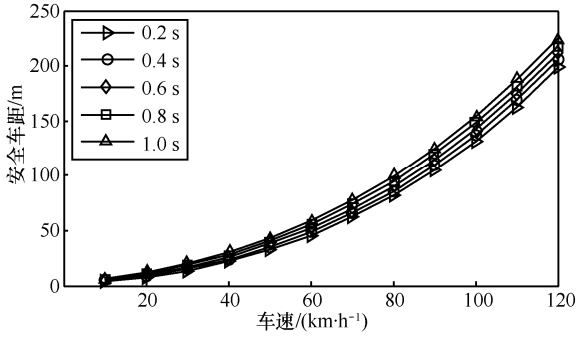

图 2 不同车速不同反应时间下的安全车距

3.2　几何交叉模型快速检测算法

根据某一时刻不同物理车辆应出现在不同物理位置的原理，认为同一时刻同一位置若出现 2 个物理车辆则说明存在声称虚假车辆的恶意行为。将网络中的车辆节点表示成一定长宽的矩形模型，同一位置 2 个物理车辆的重叠交叉检测转化为 2 个矩形的交叉识别。本文在此理论基础上，提出判别 2 个矩形交叉的几何快速识别方法检测重叠车辆，证实恶意行为的存在。

3.2.1　车辆表示

由中心点位置完全吻合来判断 2 个车辆位置接近或有一定区域重叠，要求过于严格，参考文献[11]，将车辆表示成一定长宽的车辆矩形模型，如图 3 所示。矩形的左前（LF, left front）、右前（RF, right front）、左后（LR, left rear）、右后（RR, right rear）这 4 个顶点的坐标值可根据方位角和车辆位置信息计算。

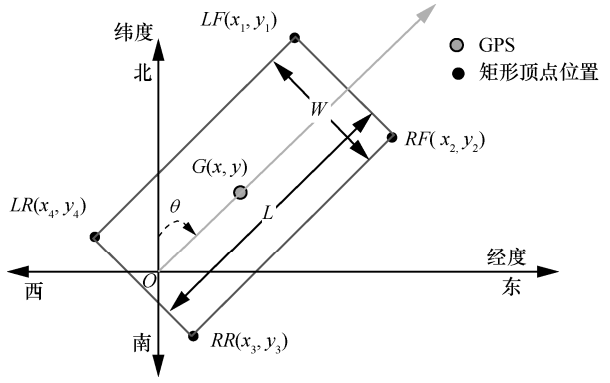

图 3　用矩形建模的车辆模型

假设车辆所在位置的方位角为 θ，GPS 测得的坐标位置 $G(x,y)$位于车辆长宽中轴线的交点，代表车辆的矩形的 4 个顶点坐标分别根据式(2)~式(9)计算。假设车辆的长宽值为(L,W)，这里取一般汽车的平均值(4,1.6)。

$$x_1 = x + \frac{L}{2}\sin\theta - \frac{W}{2}\cos\theta \tag{2}$$

$$y_1 = y + \frac{L}{2}\cos\theta + \frac{W}{2}\sin\theta \tag{3}$$

$$x_2 = x + \frac{L}{2}\sin\theta + \frac{W}{2}\cos\theta \tag{4}$$

$$y_2 = x + \frac{L}{2}\cos\theta - \frac{W}{2}\sin\theta \tag{5}$$

$$x_3 = x - \frac{L}{2}\sin\theta + \frac{W}{2}\cos\theta \tag{6}$$

$$y_3 = y - \frac{L}{2}\cos\theta + \frac{W}{2}\sin\theta \tag{7}$$

$$x_4 = x - \frac{L}{2}\sin\theta - \frac{W}{2}\cos\theta \tag{8}$$

$$y_4 = y - \frac{L}{2}\cos\theta - \frac{W}{2}\sin\theta \tag{9}$$

3.2.2　车辆几何交叉模型

车辆矩形表示后，判断 2 个车辆是否有重叠或交叉就转化为判断 2 个矩形是否重叠或交叉。

定义 1　对点矩形。若对矩形 A 的 4 个顶点分别求横坐标的最小值 $X_{\min}$ 和最大值 $X_{\max}$，以及纵坐标的最小值 $Y_{\min}$、最大值 $Y_{\max}$，得到 2 个点$(X_{\min}, Y_{\min})$、$(X_{\max}, Y_{\max})$，过这 2 个点分别作 X 轴、Y 轴的垂线，相交所构成的矩形称为原矩形的对点矩形表示为 $R\{(X_{\min}, Y_{\min})(X_{\max}, Y_{\max})\}$, $(X_{\min}, Y_{\min})$、$(X_{\max}, Y_{\max})$称为点对坐标，如图 4 所示。R 是 A 的对点矩形，A 是 R 的原矩形。

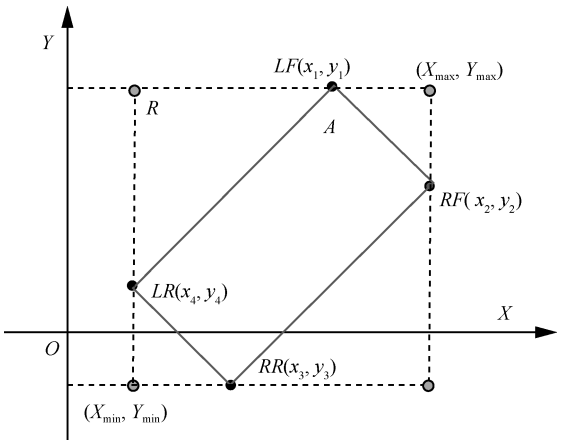

图 4　矩形 A 的对点矩形 R

由定义 1 可知，对点矩形具有各边分别平行于 X 轴、Y 轴的性质。

定义 2　对点矩形 R 的长 L_R 和宽 W_R。将对点矩形 $R\{(X_{\min}, Y_{\min})(X_{\max}, Y_{\max})\}$在 X 轴方向的投影长度称为对点矩形的长，表示为 L_R；在 Y 轴方向的投影长度称为对点矩形的宽，表示为 W_R。则长、宽分别为

$$L_R = | X_{\max} - X_{\min} | \tag{10}$$

$$W_R = | Y_{\max} - Y_{\min} | \tag{11}$$

显然，2 个对点矩形相交所得结果一定是矩形。图 5 为 2 个相交矩形的对点矩形。假设原相交矩形为 A 和 B，相应的对点矩形分别为 R_1 和 R_2，点对坐标为 $R_1\{(X_{\min}, Y_{\min})\ (X_{\max}, Y_{\max})\}$和 $R_2\{(X_{\min}', Y_{\min}')\ (X_{\max}',$

$Y_{\max}'$)}。2 个对点矩形 R_1、R_2 相交得到的矩形表示为 $Rect\{(x_{\min}, y_{\min})(x_{\max}, y_{\max})\}$，有

$$x_{\min} = \max(X_{\min}, X_{\min}') \tag{12}$$

$$y_{\min} = \max(Y_{\min}, Y_{\min}') \tag{13}$$

$$x_{\max} = \min(X_{\max}, X_{\max}') \tag{14}$$

$$y_{\max} = \min(Y_{\max}, Y_{\max}') \tag{15}$$

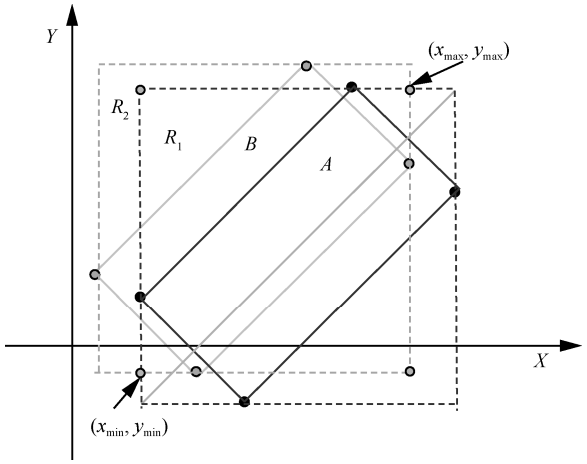

图 5 2 个相交矩形的对点矩形

若 2 个对点矩形不相交，按式(12)~式(15)计算得到的点对坐标满足式(16)，此时也能保证对点矩形对应的原矩形一定不相交，因此，将式(16)作为 2 个矩形不相交的判定条件。

$$x_{\min} > x_{\max} \,||\, y_{\min} > y_{\max} \tag{16}$$

反之，若不满足式(16)，即 $(x_{\min} \leqslant x_{\max})$&& $(y_{\min} \leqslant y_{\max})$时，不能由此立即判断 2 个矩形一定相交，而需判断 2 个对点矩形的重心距离，如果重心距离在 2 个坐标轴上的距离满足式(17)，则对点矩形对应的 2 个原矩形 A、B 相交。

$$\left(|x_{G_{R_1}} - x_{G_{R_2}}| < \frac{L_{R_1}}{2} + \frac{L_{R_2}}{2}\right) \&\& \left(|y_{G_{R_1}} - y_{G_{R_2}}| < \frac{W_{R_1}}{2} + \frac{W_{R_2}}{2}\right) \tag{17}$$

3.2.3 快速几何交叉检测算法

考虑到 GPS 定位、车辆几何建模时的长宽值等误差的存在，单次的车辆交叉并不足以证明有虚假身份的冒充行为，因此通过计算一段时间内的车辆交叉情况以提高识别的概率。一般地，安全距离 $dist_{SD}$ 不同，计算车辆交叉的时间 Δt 也不同，两者关系如式(18)所示。L 代表车辆长度，V_{AVG}^i 和 V_{AVG}^j 分别代表车距小于安全车距的 2 个车辆的平均车速。

$$\Delta t = \frac{2L + dist_{SD}}{|V_{AVG}^i - V_{AVG}^j|} \tag{18}$$

若该段时间计算的车辆交叉次数超过 1，则认为存在声称虚假位置的错误行为。结合 3.2.2 节定义的车辆几何交叉模型，提出 2 个车辆几何交叉模型检测算法，如算法 1 所示。

算法 1 2 个车辆几何交叉模型检测算法

1) 寻找车距小于最小安全车距的 2 个车辆 A 和 B，设该时刻为 t_1；

2) 交叉次数统计 $count$=0;

3) while ($|t-t_1|<\Delta t$) //t 为当前时刻

4) { 利用 CAM_A、CAM_B 中的 GPS 数据，根据式(2)~式(9)计算 A 的 4 个顶点坐标(x_1,y_1)、(x_2,y_2)、(x_3,y_3)、(x_4,y_4)以及 B 的 4 个顶点坐标(x_1',y_1')、(x_2',y_2')、(x_3',y_3')、(x_4',y_4');

5) 构造矩形 A 对应的对点矩形 $R_1\{(X_{\min}, Y_{\min})(X_{\max}, Y_{\max})\}$;

6) 构造矩形 B 对应的对点矩形 $R_2\{(X_{\min}', Y_{\min}')(X_{\max}', Y_{\max}')\}$;

7) 根据式(12)~式(15)求 R_1 和 R_2 的相交矩形 $Rect\{(x_{\min}, y_{\min})(x_{\max}, y_{\max})\}$;

8) if $((x_{\min} \leqslant x_{\max})$ && $(y_{\min} \leqslant y_{\max}))$

9) $L_{R_1} = |x_{\max} - x_{\min}|$; $W_{R_1} = |y_{\max} - y_{\min}|$;

10) $L_{R_2} = |x_{\max}' - x_{\min}'|$; $W_{R_2} = |y_{\max}' - y_{\min}'|$;

11) if $\left(|x_{G_{R_1}} - x_{G_{R_2}}| < \frac{L_{R_1}}{2} + \frac{L_{R_2}}{2}\right) \&\& \left(|y_{G_{R_1}} - y_{G_{R_2}}| < \frac{W_{R_1}}{2} + \frac{W_{R_2}}{2}\right)$

12) {A、B 交叉; $count$++}

13) else A、B 不交叉;

14) }

15) else A、B 不交叉;

16) }

17) if ($count$ > 1) 存在虚假行为;

3.3 基于位置偏差矩阵的 Sybil 节点识别

快速几何交叉检测算法只能证实虚假车辆的存在，但无法确定谁是真正的虚假车辆，为此，提出根据证实车辆动态收集邻居信息建立局部车辆位置偏差矩阵并识别真假车辆的方法。

3.3.1 位置偏差矩阵建立

若证实车辆 N_c 有 n 个邻居节点 $N_1, N_2, \cdots, N_n$，对应的编号为 $1,\cdots,n$，t 时刻各邻居节点发送的邻居观察为 Obs_i^t ($i \in 1,\cdots,n$)，参考文献[25]可建立 t 时刻下的 n 阶观察矩阵 $\boldsymbol{M}_o^t$ 和 n 阶估算矩阵 $\boldsymbol{M}_e^t$。矩阵中

的行/列号 i 对应编号为 i 的邻居节点。观察矩阵存储了 t 时刻 n 个邻居节点间是否能直接观察彼此的状态关系，如果节点 N_i 能观察节点 N_j，则表示节点 N_j 出现在节点 N_i 的 Obs_i^t 中，此时 $\boldsymbol{M}_{\mathrm{o}}^t(i,j)$ 位置上的元素值为 1。$\boldsymbol{M}_{\mathrm{o}}^t$ 中的矩阵元由式(19)确定。

$$\boldsymbol{M}_{\mathrm{o}}^t(i,j)=\begin{cases}1, \text{节点} N_i \text{ 能观察节点} N_j\\ 0, \text{节点} N_i \text{ 不能观察节点} N_j\end{cases} \tag{19}$$

节点本身不会出现在自身的邻居观察中，故该矩阵中对角线上的元素值全为 0。由于无线信道的不稳定性，同一时刻 2 个节点不一定能相互观察，因此该矩阵是非对称矩阵。

估算矩阵由节点的估算距离确定，d_{ij}^t 代表 t 时刻节点 N_i 和节点 N_j 之间的估算距离，R 代表节点的通信半径。若 $d_{ij}^t \leqslant R$，则 $\boldsymbol{M}_{\mathrm{e}}^t(i,j)$ 位置上的元素值为 1，否则为 0，如式(20)所示。

$$\boldsymbol{M}_{\mathrm{e}}^t(i,j)=\begin{cases}1, d_{ij}^t \leqslant R\\ 0, d_{ij}^t > R\end{cases} \tag{20}$$

对观察矩阵和估算矩阵作异或运算可进一步定义位置偏差矩阵 $\boldsymbol{M}_{\mathrm{d}}^t$。

$$\boldsymbol{M}_{\mathrm{d}}^t=\boldsymbol{M}_{\mathrm{o}}^t \oplus \boldsymbol{M}_{\mathrm{e}}^t \tag{21}$$

其中，$\oplus$ 表示异或运算。只有当观察方阵和估算方阵中对应位置(i, j)上元素都为 0 或都为 1 时，偏差矩阵中相应位置(i, j)的元素才为 0，这代表时刻 t 邻居观察和估算位置是一致的，否则，代表不一致，存在异常现象。

3.3.2　Sybil 节点识别

为了由偏差矩阵识别 Sybil 节点，可纵观所有邻居节点对某一节点的位置观察，在位置偏差矩阵中某一列上的值代表了其他各节点对该列所代表节点的观察，因此定义如式(22)所示的偏差度量值。

$$D_i^t=\sum_{k=1}^{n}\boldsymbol{M}_{\mathrm{d}}^t(k,i) \tag{22}$$

其中，D_i^t 表示所有邻居节点某一时刻对编号为 i 的节点位置一致性观察值。

将证实车辆视为局部范围内的中心车辆，收集各节点的邻居观察，当证实车辆检测到局部范围内 2 个车辆交叉时，开始建立对应时刻的位置偏差矩阵 $\boldsymbol{M}_{\mathrm{d}}^t$。对交叉的 2 个节点 N_i 和 N_j 查找 $\boldsymbol{M}_{\mathrm{d}}^t$，计算各自的偏差度量值 D_i^t 和 D_j^t，根据两者的比较结果确定 Sybil 节点。显然，对发生交叉的 2 个节点，偏差度量值均为 0 的情形不可能存在；若两者中只有一值为 0，则值不为 0 的另一节点便为 Sybil 节点；若两者均不为 0，则偏差度量值较大的为 Sybil 节点。基于位置偏差矩阵的 Sybil 节点识别算法（PDM，Sybil-recognition algorithm based on position deviation matrix）如算法 2 所示。

算法 2　基于位置偏差矩阵的 Sybil 节点识别算法

1) 由邻居节点的邻居观察，根据式(19)建立观察矩阵 $\boldsymbol{M}_{\mathrm{o}}^t$；

2) 计算邻居节点间的估算距离，根据式(20)建立估算矩阵 $\boldsymbol{M}_{\mathrm{e}}^t$；

3) 根据观察矩阵和估算矩阵，根据式(21)建立位置偏差矩阵 $\boldsymbol{M}_{\mathrm{d}}^t$；

4) 对于交叉节点 N_i 和节点 N_j，根据式(22)分别求出 D_i^t 和 D_j^t；

5) if ($D_i^t < D_j^t$)　/*包含了一个为 0，另一个不为 0 以及两者均不为 0 的情况*/

6)　　N_j 为 Sybil 节点；

7) else if ($D_i^t > D_j^t$)

8)　　N_i 为 Sybil 节点。

4　算法分析和仿真验证

4.1　算法分析

本文所提检测方法由识别虚假行为的 GCR 算法和识别 Sybil 节点的 PDM 算法这 2 部分组成，因此分别对这 2 部分计算开销和检测性能。

4.1.1　计算开销

1) 交叉识别的开销

在证实车辆的单跳邻居范围内未发现在彼此安全车距内的车辆时，不执行交叉识别算法，否则，利用构造对点矩形求相交矩形，通过比较对点矩形顶点坐标的最小和最大值等简单操作完成 2 个车辆交叉识别，因此，单次的交叉识别过程开销为 $O(1)$。

2) Sybil 节点识别开销

证实车辆 N_c 通过收集的邻居节点信息建立邻居节点间位置偏差矩阵，假设 t 时刻 N_c 的单跳邻居车辆节点数目是 n，则建立 n 阶位置偏差矩阵的计算开销为 $O(n^2)$。识别 Sybil 节点的过程是对 2 个交叉车辆 N_i 和 N_j 分别在 n 阶位置偏差矩阵上求第 i 列和第 j 列的元素之和，此过程的计算开销为 $O(n)$。

综上，整个检测算法中单次交叉识别和 Sybil 节点识别总计算开销为 $O(n)$；此外，整个算法除在特定的事件驱动下启动外，不会产生额外的通信开销，且无需特定硬件的支持，是一种事件驱动的轻量级检测方法。

4.1.2 检测性能

1) 交叉识别检测

无论有无定位误差，恶意节点伪造的 Sybil 节点由于不真实存在总能与经过的真实车辆发生交叉而被检出，但如果存在 GPS 定位误差时，真实车辆的定位误差可能会引起真实车辆间的伪交叉，造成对真实车辆的误判。

2) Sybil 节点检测

2 个交叉节点的 Sybil 识别取决于周围邻居节点的位置一致性观察，设 t 时刻证实车辆 N_c 检测到 2 个节点 N_x 和 N_y 交叉，在不考虑 GPS 误差的情况下，一般认为是真实车辆与另一恶意车辆 N_m 伪造的虚假车辆相交，此时定理 1 成立。

定理 1 若存在节点 N_b，满足以下 2 种情形之一，则能识别出 2 个交叉节点中的 Sybil 节点：1) N_b 是证实节点 N_c 和恶意节点 N_m 的公共邻居节点，但不是交叉位置的邻居节点；2) N_b 是证实节点 N_c 和交叉位置的公共邻居节点，但不是恶意节点 N_m 的邻居节点。

证明 当证实节点 N_c 检测到交叉时，建立以 N_c 为中心的局部位置偏差矩阵 $\boldsymbol{M}_{\mathrm{d}}^{t}$，考察 N_b 对 2 个交叉节点的观察值和估算距离，因 2 个交叉节点物理位置接近，故 N_b 与交叉位置的估算距离 d_{N_b,N_x} 和 d_{N_b,N_y} 相近，有 $\boldsymbol{M}_{\mathrm{e}}^{t}(N_b,N_x)=0$ 及 $\boldsymbol{M}_{\mathrm{e}}^{t}(N_b,N_y)=0$。

若满足情形 1)，由于 N_b 不是交叉位置的邻居节点，若该位置的节点为真实节点，则 N_b 不能接收来自该真实节点发送的消息，对其是不可观察的，观察矩阵 $\boldsymbol{M}_{\mathrm{o}}^{t}$ 对应的元素值为 0；若该位置的节点为恶意节点 N_m 伪造的虚假节点，因 N_b 是 N_m 的邻居节点，能接收虚假节点发送的消息，对其是可观察的，观察矩阵对应的元素值为 1，显然，此时该交叉节点的观察值和估算距离不一致，对应的位置偏差矩阵中元素为 1，因此被识别为 Sybil 节点。

情形 2)的证明与此类似。

由定理 1 知，在 GPS 零误差的情况下，Sybil 节点的检测率取决于 N_b 节点的存在概率；进一步，该定理也可推广应用到 GPS 有定位误差时的情况。

4.2 仿真验证

4.2.1 环境设置

VANET 中的车辆交通运动场景由 SUMO[29]产生，SUMO 是一款专业的开源微观交通仿真平台，其中所需的路网和路径等 xml 文件使用 MOVE[19]配置得到。本文模拟双向共 6 车道的高速公路环境，在 8 km 的道路上生成接近真实车辆驾驶的车辆位置、速度等实验场景数据，形成一定的 trace 文件，之后载入 NS-2 网络模拟器，读取 trace 文件中不同时刻下不同车辆的位置、速度等数据，生成车辆节点，按设定的通信参数模拟 VANET 中车与车之间的网络通信并执行检测算法，实验结果在 Matlab 中显示。实验参数分交通场景和网络通信这 2 个部分，如表 2 所示。

表 2 实验参数设置

类别	参数名	参数值
交通场景	车道数	6
	道路长度/km	8
	车道宽度/m	3.5
	车辆速度/(km·h^{-1})	40~120
网络通信	车辆通信半径/m	250
	通信周期/s	1
	MAC 层协议	802.11p

4.2.2 实验结果及分析

为验证算法的有效性，定义了检测率和误检率这 2 个度量值。检测率是指成功检测 Sybil 节点的比例；误检率是指真实车辆被误认为是 Sybil 节点的比例。同时，为了削减证实车辆 N_c 邻居节点出现位置的随机性对检测结果的影响，对不同场景仿真多次求出平均结果。

1) 安全车距对算法影响

整个算法在安全车距的驱动下执行，因此算法执行性能与此息息相关，实验中，选用 SUMO 仿真平台，车辆间的安全车距通过车辆跟车模型中的 mingap 参数来设置，此参数一旦设定，车辆的跟车距离将保持在设定的 mingap 值之外，无法驶入安全车距内形成车辆的模拟交叉。但由 3.1 节分析可知，车速是影响安全车距的最主要因素，此外，车辆的行驶速度也间接反映了道路的通行状态，由广义 Greenshield 模型[28]可知，车速 v 与道路通行状态指示值车辆密度 Q 之间存在如式(23)所示的关系，其中，v_f 为车辆的自由流速度，即交通密度

Q 趋于 0 时的车速，Q_j 为道路达到拥堵时的车辆密度。

$$v = v_f - \frac{Q}{Q_j} v_f \tag{23}$$

综合车辆密度、车速和安全车距三者关系得：道路上车辆密度较小时，车速较高、安全车距较长；反之，车辆密度较大时，车速较低、安全车距较短。车辆密度在 SUMO 平台中可通过车流控制来实现，因此，在实验中研究安全车距对算法的影响时，转化成不同车辆密度对算法执行性能的影响。

2) 检测率和误检率

在 GPS 零误差的理想状态下，整个算法的检测性能与网络中证实车辆的邻居节点分布有关。实验首先测量了不同场景即不同车辆密度下网络中节点的邻居节点数情况，得到如图 6 所示的直方图。在同一车辆密度下，由于是对多个车辆不同时刻的邻居节点数目求平均，因此不同时刻的邻居节点数目偏差不大，当车辆密度 Q=90 vel·km^{-1}·ln^{-1}，平均车速为 100 km·h^{-1} 时，车辆的平均邻居节点数为 20 左右。在不同车辆密度时，邻居节点数目随车辆密度的增加而增加。

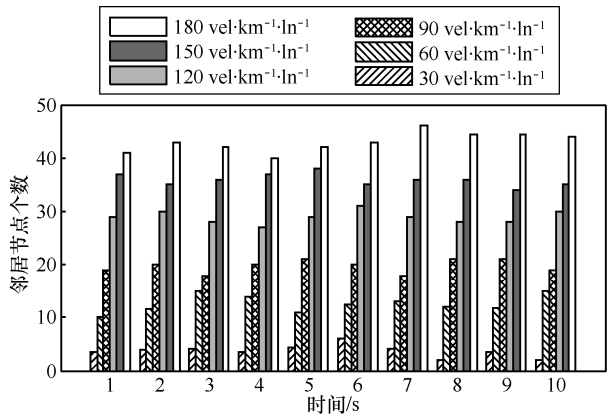

图 6　网络中不同时刻不同密度下节点的平均邻居节点数目

在 SUMO 中通过车流来控制网络中的车辆密度，在 8 km 的实验仿真路段上，每 0.25 km 随机选择 1 辆车辆作为证实车辆，再在其余的节点中随机选择 5%的节点作为恶意节点，并成功伪造一些虚假位置以产生 Sybil 节点，每个恶意节点与伪造出的 Sybil 节点之间位置偏差超过车辆的 GPS 定位误差范围；为得到合理误差范围内的位置数据，从 trace 文件读取 t 时刻车辆 N_i 的位置值(x_i^t, y_i^t)，在以(x_i^t, y_i^t)为圆心、ΔGPS（GPS 的绝对误差，单位 m）为半径的圆上随机生成新的数据值（$x_i^{t'}, y_i^{t'}$），作为某时刻车辆 N_i 的误差的位置数据。

检测率。观察 500 s 内 8 km 的实验仿真路段上不同车辆密度下的检测情况，由图 7 可知，无论有无 GPS 误差，Sybil 节点的检测率总体趋势是随网络中车辆密度的增加（即安全车距的减少）而提高的，这是因为当车辆密度增加时，车辆交叉的可能性增大，且对于相交的 2 个车辆，邻居观察车辆数目就越多，因此对虚假车辆位置不一致性的观察就越多，识别率提高。当车辆密度达到 90 vel·km^{-1}·ln^{-1}，车速平均为 100 km·h^{-1}，即达到车辆常态运行速度时，检测率稳定在 95%以上。

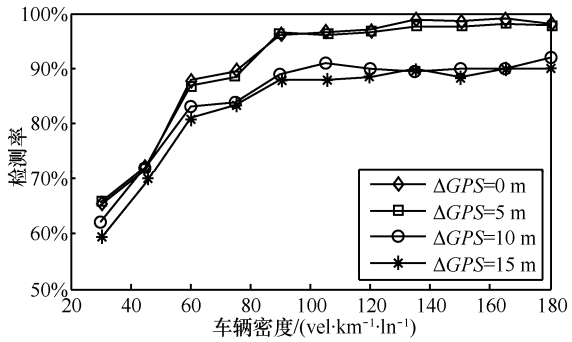

图 7　检测率随车辆密度的变化情况

在考虑车辆 GPS 误差时，Sybil 节点检测情况也不相同，ΔGPS=5 m 时的检测率与 ΔGPS=0 m 时接近，原因在于：此时 GPS 误差引起的位置偏移量较小，位置的偏差估算影响甚小。当 GPS 误差相对较大时，检测率下降，因为 GPS 误差引起了一定的位置偏移，产生位置的不一致性，恶意车辆伪造的虚假车辆除可能与真实车辆交叉外，也可能与真实车辆的误差位置相交，此时相当于 2 个虚假车辆相交，两者均有位置偏差，识别 Sybil 节点的漏检情况会降低算法的检测率。

误检率。位置相关的 Sybil 节点检测方法中，车辆位置信息的获取由 GPS 定位系统确定，由于 GPS 定位误差的存在，导致真实车辆的误差位置可能与其他真实车辆发生相交从而造成误判，因此，在观察检测率的同时对系统的误检情况进行分析，得到如图 8 所示不同车辆密度下的误检率情况。当 ΔGPS=5 m 时，误检率几乎为 0，因为此时位置偏差较小，误差位置与真实车辆交叉的概率极低。当 GPS 误差增大时，误检率增大，且随着车辆密度的增大逐渐趋于稳定。车辆 GPS 误差增大时产生的位

置偏移增大，被认为是位置不一致节点的概率增大，误检率升高。随着车辆密度的增加，定位误差引起的“虚假”车辆与真实车辆的交叉能被更多的邻居车辆所观察，且当车辆密度达到一定值时，检测节点 N_b（如定理 1 所示）的存在概率较大，误检率趋于稳定。但“虚假”车辆位置相对恶意节点制造的虚假位置偏差值较小，且误差位置的出现本身具有一定概率性，因此总的识别率相对正常节点与恶意节点伪造的虚假节点的交叉识别较低。

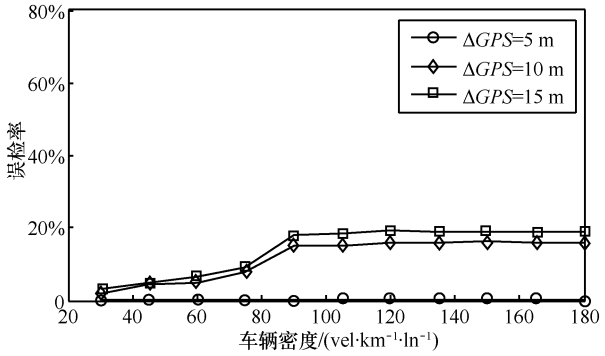

图 8 误检率随 GPS 定位误差变化

检测开销。为了分析算法的快速识别性能，同样设置了不同的车辆密度场景，在其中随机选择 1 个车辆作为恶意车辆，并产生 2 个 Sybil 节点，观测不同场景下，识别 Sybil 节点过程的处理时延。每个场景重复多次得到的实验结果如图 9 所示，并与文献[22]的方法对比。

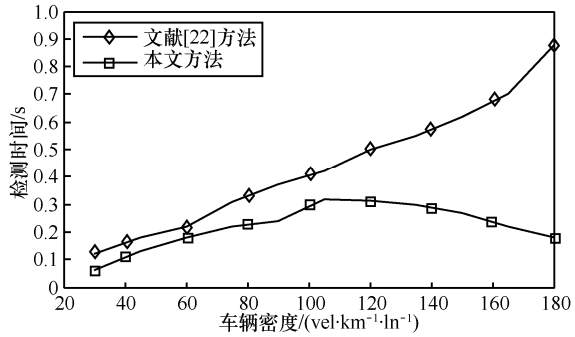

图 9 不同车辆密度下的处理时延比较

文献[22]的方法检测时间随密度几乎呈直线增长，本文方法的检测时间随密度增长呈类正态曲线分布。这是因为文献[22]中检测时间直接受检测区域内节点数目的影响，当节点数目增加时，检测开销随之增加；本文方法 Sybil 节点的快速识别主要受证实车辆邻居节点数及节点安全区域内车辆数影响，图 6 显示了不同车辆密度下的邻居节点数分布情况，随着车辆密度的增加，邻居节点数也逐渐增长，但此时车速逐渐减慢，安全距离随之减小；在车辆密度加大安全车距减小的情况下安全区域内的车辆数呈现先增后减的趋势，因此，Sybil 节点的快速交叉识别过程呈现了同样的趋势，在车辆密度达到 110 $vel\cdot km^{-1}\cdot ln^{-1}$、车速为 90 $km\cdot h^{-1}$ 时网络中的处理时延最大，为 0.3 s 左右，不会影响节点间正常通信时周期性 CAM 的发送，且车辆的定位精度不会影响算法的检测开销。

此外，与文献[22]相比，本文仅利用节点间周期性发送的 CAM，对其中的位置信息进行处理以识别车辆的虚假信息，减少了网络中通信信息的种类要求，同时安全区域的定义避免了车辆密度过大对网络造成的通信负载影响，对 CAM 的处理时延较低，符合车联网环境下的实时性要求[20] ，是一种轻量级的识别算法。

5 结束语

对伪造不同位置信息同时声称多个身份的 Sybil 攻击，将虚假身份的识别转化为验证车辆所处位置的真实性，当车辆出现在另一车辆的安全区域内时，启动快速识别 2 个车辆是否重叠的几何交叉模型算法，检测声称虚假位置信息的错误行为；同时根据邻居范围内的局部车辆，建立位置偏差矩阵，实现识别 Sybil 节点的 PDM 算法。性能分析和仿真实验表明，安全区域驱动下的轻量级算法识别速度快，检测率高，在车辆定位误差较低时性能更好；安全区域的引入，同时也均衡了车辆密度过大时造成的通信负载影响，与同类算法相比，通信处理时延较低。

从实验结果也可看出，车辆位置信息精度对检测结果有一定影响，因此，较高的车辆定位精度是提高 Sybil 攻击检测率的前提，车辆高精度定位技术是下一步继续研究的方向。

参考文献：

[1] HARTENSTEIN H, BOCHOW B, EBNER A, et al. Position-aware ad hoc wireless networks for inter-vehicle communications: the FleetNet project[C]//ACM MobiHoc 2001. 2001: 259-262.

[2] ENKELMANN W. FleetNet-applications for inter-vehicle communication[C]//IEEE Intelligent Vehicles Symposium. 2003: 162-167.

[3] MEJRI M N, BEN-OTHMAN J, HAMDI M. Survey on VANET security challenges and possible cryptographic solutions[J]. Vehicular communications, 2014,1(2): 53-66.

[4] TRULLOLS O, FIORE M, CASETTI C, et al. Planning roadside infrastructure for information dissemination in intelligent transportation systems[J]. Computer Communications, 2010, 33 (4):432-442.

[5] GEORGIOS K, ONUR A, EYLEM E, et al. Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions[J]. IEEE Communications Surveys and Tutorials, 2011, 13(4): 584-616.

[6] WAHAB O A, MOURAD A, OTROK H, et al. CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks[J]. Expert Systems with Applications, 2016, 50: 40-54.

[7] XIAO B, YU B, GAO C S. Detection and localization of Sybil nodes in VANETs[C]//2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks. 2006: 1-8.

[8] CHEN C, WANG X, HAN W L, et al. A robust detection of the Sybil attack in urban VANET[C]//The 29th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS 2009). 2009:270-276.

[9] CHANG S, QI Y, ZHU H, et al. Footprint: detecting Sybil attacks in urban vehicular networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(6): 1103-1114.

[10] SOYOUNG P, BABER A, DAMLA T, et al. Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support[J]. Security and Communication Networks, 2013, 6(4): 523-538.

[11] JIN D X, SONG J. A traffic flow theory aided physical measurement-based Sybil nodes detection mechanism in vehicular ad hoc networks[C]//2014 IEEE/ACIS 13th International Conference on Computer and Information Science. 2014: 281-286.

[12] GUETTE G, DUCOURTHIAL B. On the Sybil attack detection in VANET[C]//IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS 2007). 2007:1-6.

[13] YU B, XU C Z, XIAO B. Detection Sybil attacks in VANETs[J]. Journal of Parrel and Distributed Computing, 2013: 746-756.

[14] HICHEM S, MOHAMMED S S. An accurate and efficient collaborative intrusion detection framework to secure vehicular networks[J]. Computers & Electrical Engineering, 2015, 43(c):33-47.

[15] GROVER J, GAUR M S, LAXMI V, et al. A Sybil attack detection approach using neighboring Vehicles in VANET[C]//The 4th International Conference on Security of Information and Networks. 2011: 151-158.

[16] GROVER J, LAXMI V, GAUR M S. Sybil attack detection in VANET using neighboring vehicles[J]. International Journal of Security and Networks, 2014, 9(4): 222-233.

[17] SCHMIDT R K, LEINMUELLER T, SCHOCH E, et al. Vehicle behavior analysis to enhance security in VANETs[C]//The 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008). 2008: 1-8.

[18] STUEBING H, JAEGER A, BIßMEYER N, et al. Verifying mobility data under privacy considerations in Car-to-X communication[C]// 17th ITS World Congress 2010. 2010:1-12.

[19] RAMON B, JAVIER G, SORIANO S, et al. Road traffic congestion detection through cooperative vehicle-to-vehicle communications[C]// 4th IEEE Workshop On User Mobility and Vehicular Networks (On-MOVE 2010). 2010: 606-612.

[20] KARNADI F K, MO Z H, LAN K. Rapid generation of realistic mobility models for VANET[C]//Wireless Communications and Networking Conference. 2007: 2506-2511.

[21] ETSI TS 102 637-2 V1.2.1. Specification of cooperative awareness basic service[S]. 2011.

[22] 李春彦, 刘怡良, 王良民. 车载自组网基于交通场景的入侵行为检测机制[J]. 山东大学学报, 2014, 44(1): 29-34.
LI C Y, LIU Y L, WANG L M. Intrusion detection scheme based on traffic scenarios in vehicular ad hoc networks[J]. Journal of Shandong University, 2014, 44(1):29-34.

[23] ABUELENIN S M, ABUL-MAGD, et al. Effect of minimum headway distance on connectivity of VANET[J]. Elsevier GmbH, 2015, 69(5): 867-871.

[24] BERLIN M A, MUTHUSUNDARI S. Safety distance calculation for collision avoidance in vehicular ad hoc networks[J]. Scholars Journal of Engineering and Technology (SJET), 2016, 4(1): 63-69.

[25] WEI Y W, GUAN Y. Lightweight location verification algorithms for wireless sensor networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(5): 938-950.

[26] LABAYRADE R, ROYERE C, AUBERT D. Experimental assessment of the RESCUE collision-mitigation system[J]. IEEE Transactions on Vehicular Technology, 2007, 56(1): 89-102.

[27] CHEN Y J, CHEN C C, WANG S N, et al. GPSenseCar-A collision avoidance support system using real-time GPS data in a mobile vehicular network[C]//Second International Conference on Systems and Networks Communication. 2006.

[28] KAMRAN Z, MILOS B, MILOJEVIC, et al. Host-based intrusion detection for VANETs: a statistical approach to rogue node detection[J]. IEEE Transactions on Vehicular Technology, 2016, 65(8): 6703-6714.

[29] KRAJZEWICZ D, HERTKORN G, RÖSSEL C, et al. SUMO (simulation of urban mobility): an open-source traffic simulation[C]//4th MESM. 2002: 183-187.

作者简介：

辛燕（1978-），女，江苏泰兴人，江苏大学博士生，主要研究方向为车联网安全。

冯霞（1983-），女，江苏扬中人，安徽大学博士生，主要研究方向为车联网与交通大数据安全。

李婷婷（1993-），女，江苏南通人，江苏大学硕士生，主要研究方向为车联网安全与隐私保护。