doi:10.11959/j.issn.1000-436x.2016156

基于弱分类器集成的车联网虚假交通信息检测

刘湘雯[1]，石亚丽[1]，冯霞[2]
（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 230000）

摘 要：车联网中车辆以自组织的方式相互报告交通信息，开放的网络环境需要甄别消息，然而，要快速移动的车辆在短时间内检测出大量的交通警报信息是非常困难的。针对这一问题，提出一种基于弱分类器集成的虚假交通信息检测方法。首先，扩充交通警报信息的有效特征，并设计分割规则，将信息的特征集划分为多个特征子集；然后，根据子集特征的不同特性，使用对应的弱分类器分别进行处理。仿真实验和性能分析表明，选用弱分类器集成方法检测车联网中的虚假交通信息减少了检测时间，且由于综合特征的应用，检测率优于仅使用部分特征的检测结果。

关键词：车联网；虚假信息检测；弱分类器集成；BP 神经网络
中图分类号：TP393 **文献标识码**：A

False traffic information detection based on weak classifiers integration in vehicular ad hoc networks

LIU Xiang-wen[1], SHI Ya-li[1], FENG Xia[2]
(1. School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China;
2. Information Assurance Technology Collaborative Innovation Center, Anhui University, Hefei 230000, China)

Abstract: Vehicles report traffic information mutually by self-organized manner in vehicular ad hoc networks (VANET), and the message need to be identified in the open network environment. However, it is very difficult for fast moving vehicles to detect a lot of traffic alert information in a short time. To solve this problem, a false traffic message detection method was presented based on weak classifiers integration. Firstly, the effective features of traffic alert information was extended and segmentation rules were designed to divide the information feature set into multiple feature subsets, then the corresponding weak classifiers were used to process feature subsets respectively according to the different characteristics of the subsets' features. Simulation experiments and performance analysis show that the selected weak classifiers integration method reduces the detection time, and because of the application of combined features, the detection rate is better than the test of using only some of the characteristics.

Key words: VANET, false information detection, weak classifiers integration, BP neural network

1 引言

随着移动通信技术、物联网和无线传感网络技术的广泛应用，车联网逐渐成为智能交通的有效途径之一[1]。车联网可为车辆提供交互通信功能，通过信息的共享和及时发布，在事故预警、保障交通安全以及为用户提供舒适的驾驶环境等方面起到巨大的作用[2]。在交通安全应用中，车联网中的车辆节点向邻居车辆广播交通信息，如车辆位置、速度、加速度等，提前告知道路状况，从而降低交通阻塞带来的时间和资源的浪费，提高交通安全[3]。然而，车联网处于开放环境，无法排除恶作剧用户、

收稿日期：2015-11-09；**修回日期**：2016-07-04
基金项目：国家自然科学基金资助项目（No.61472001）；江苏省自然科学基金资助项目（No.BK2011464）；江苏省青蓝工程基金资助项目；镇江市工业支撑基金资助项目（No.GY2013030）
Foundation Items: The National Natural Science Foundation of China (No.61472001), The Natural Science Foundation of Jiangsu Province (No.BK2011464), Blue Project of Jiangsu Province, Zhenjiang City Industrial Support Project(No.GY2013030)

软硬件损坏或恶意入侵情况的存在，已知的攻击种类包括位置伪造[4]、信息的窃听、篡改[5]、抑制[5]、重放[6]以及数据分组拘留[6]等攻击方式，导致交通警报信息被修改、延迟、丢弃，甚至损害到车联网应用带来的效益，危害驾乘者的生命财产安全，造成更严重的交通事故。为此，检测虚假信息以确保交通信息的真实性，成为车联网安全驾驶的重要方面。

对车联网中虚假警报信息的检测方案主要有 2 类。1) 判断节点是否异常。这类方案的基本假设为“异常节点发出的信息一定是虚假的”，通过节点间的信息交互实现对信息源节点的判断。其优点是检测方法简单，对处理器的计算能力要求低，适用于快速实时计算能力相对较低的车联网环境，但此类方案对正常节点与恶意节点相对数量要求较高，只有当正常节点的数目多于异常节点时，才能充分发挥较好的性能；如果网络中存在数量上相近或者局部占优的恶意节点，会导致该方法整体失效，对消息的判断准确率也大大降低[7]。如一个信任度较高的节点恰好发出了一条虚假信息。2) 基于警报信息自身的特征进行虚假信息的分类研究[8]。这类方案输入的警报信息特征越多，识别的效率越高，其缺点是识别算法复杂度较高，警报信息很多时，计算导致的时延往往会损害警报信息的时效性。更为重要的是，车联网的应用往往在高密度或者高速度的交通场景下，出于对提前预报的需求，网络信息的覆盖范围及网络规模通常较大，每个节点都会接受并处理大量其他车辆发送的警报信息。通常而言，基于节点行为判断的方案通信负荷会过大，而基于预警信息特征的方案，由于计算负荷较大，会导致较大的时延，从而降低车联网所提供的交通信息预警效果。

本文提出一种基于弱分类器集成的虚假交通信息检测方法。该方法首先扩充警报信息包含的特征值，如将发送者的特征（车辆信誉值、信息发送时车辆节点所在的位置等）作为消息分组的一部分；然后根据警报信息丰富的综合特征，检测预警信息的真假。为提高检测效率，将综合特征分割成若干特征子集，利用不同的弱分类器对部分特征子集并行处理，并将处理结果集成，根据警报事件的可信度进行二次判断。方法的主要特点如下。

1) 将丰富的节点特征包含在消息分组中，融合了节点信息和消息信息双重特征，为检测率的提高提供了足够的信息特征。

2) 新型分组虽然增加了单次分组传输的通信代价，但是减少了基于节点识别的通信次数，从而降低了检测的整体通信代价。

3) 采用多个弱分类器并行处理的方法，降低了计算代价，虚假警报检测的时效性得到充分保证，同时还提高了检测率。

2　相关工作

现有的关于车联网虚假警报信息检测方案主要分为对节点行为异常的判断和对警报信息特征的分类研究。前者采用的主要方法有基于信任机制和基于投票机制 2 种；而后者的研究主要以数据为中心，集中在设计计算能力低且识别效果好的分类器以及通过各种渠道获取丰富的警报信息特征上。

基于信任机制[8~11]的方法根据车辆信誉值的高低来判别该车辆是否提供虚假交通信息。Abdelaziz 等[8]提出有效的信任模型，根据上一个转发节点的观点和接收消息的验证延迟来检测和撤销不诚实的节点以及控制恶意数据，并引入同伴车辆的概念确定最短和最信任的路径传递数据分组。Ding 等[9]提出基于事件的信誉模型过滤虚假警报消息，该方法将遇到相同事件的所有车辆分为不同角色，采用动态的基于角色的信誉评估机制来决定交通信息是否可信。Zhang 等[10]提出一种车联网中基于信任模型的消息评估和传播框架，该框架在消息传播过程中，主动检测恶意信息，使用一系列的信任度量指标，包括同伴车辆的信任关系、信任意见、基于经验的信任度、基于角色的信任度等，对同伴车辆节点间共享的信息质量进行建模。Shaikh 等[11]则针对不同节点发出的关于同一事件的消息，利用接收节点计算所有消息信任值，并接收信任值最大的那条消息为真实信息，实现对车辆网中具有匿名身份的车辆节点的信任管理。

基于投票机制[12,13]的方法中，Ostermaier 等[12]提出基于信息中心评估危害信息的可信性的安全机制，该方法用 4 种投票机制来判断当地危险警告。Li 等[13]提出一种基于不同交通场景的混合式入侵行为检测机制，当车辆不在同一道路上行驶时，使用局部投票的 VOTE 方法进行入侵检测。

上述方法以车辆节点为中心，对 RSU 和信誉度高的节点的依赖程度大，导致虚假警报信息的检测效率较低。因此，一部分研究者提出以数据为中

心的基于警报信息特征的检测方案。如 Kim 等[14]利用丰富的互补信息来源构建多源检测模型，信息源包括加密认证、事件位置、当地传感器、其他车辆反应行为、RSU 验证、发送者的信任值。该模型结合各种不同来源的信息计算事件信任值，并根据事件距离接收者位置的远近设置阈值，当事件信任值超过阈值时，OBU 才会触发警报通知驾驶者。Zhang 等[15]则通过设计高效的分类器识别虚假信息，提出一种车联网中基于增量学习的 BP 神经网络的虚假消息过滤器。为提高识别精度，该方法采用 2 层过滤机制——粗过滤和细过滤。粗过滤通过数字签名、时间、地理位置以及 RSU 对信息的支持这些特征来判断消息的真实性；细过滤将车联网交通信息中发送者与接收者之间的距离、事件与发送者之间的距离、发送者当前速度、发送者的信誉值等特征作为输入量，由神经网络分类器给出是否为虚假信息的判断。Zhang 等[15]以信誉值作为辅助，首次提出使用 BP 神经网络直接对警报信息进行检测，比以节点为中心的检测方法针对性更强，并通过实验验证了该方法对虚假警报信息的过滤效果更好。

表 1 对上述几种方法进行了归纳，比较其优缺点并进行综合分析。在此基础上，提出一种基于弱分类器集成的虚假交通信息检测方法，首先，增加警报信息中的节点特征，并对特征分类；然后，在基于信息特征检测的方法中，用适合各类特征特点的弱分类器集成方法，实现更多特征、更低计算代价和更高检测率的综合性能。

3　模型与概念定义

3.1　系统模型与假设

本文采用典型的 VANET 系统模型（如图 1 所示）。该系统模型主要包含 3 个实体：可信权威机构（TA，trust authority）、固定在路边的基础设施（RSU，road-side unit）和配备在车辆上的车载单元（OBU，on-board unit）。各实体的主要功能如下。

1) TA：TA 主要负责为网络中的 RSU 和 OBU 发布密钥信息。车辆发送的交通信息需要经过密钥签名以实现对虚假信息发布者的认证，并防止真实信息被恶意车辆篡改。

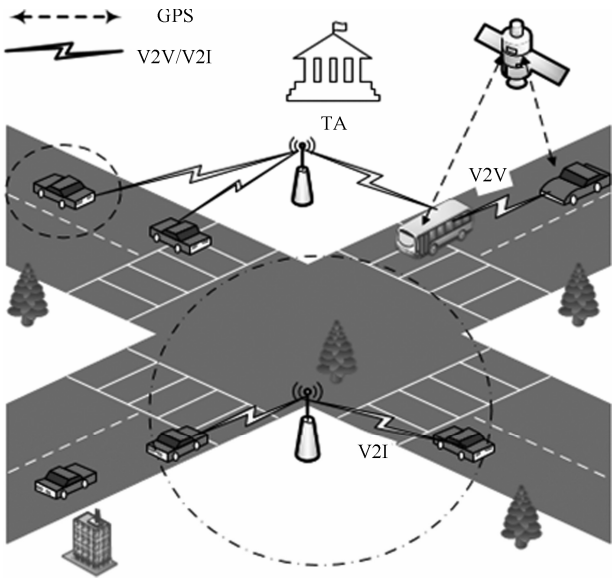


图 1　VANET 系统模型

2) RSU：RSU 主要负责向其通信范围内的车辆发布信息，通常认为 RSU 自主发布的信息是真实可信的，可以作为虚假信息检测的依据。同时，RSU 也负责对车辆和 TA 的信息进行存储转发。RSU 还可以在空闲情况下，对接收的交通信息进行虚假检测。

3) OBU：OBU 主要负责发布交通信息，它可以通过 V2V 或 V2I 的方式进行通信。同时，OBU 是虚假信息检测的主要实体。

本文采用了与文献[8]相似的安全假设。

假设 1：车辆都配备 GPS 设备、前后向红外线雷达（假设雷达扫描半径为 200 m）、红外线信号接收设备、无线信号收发器以及各种传感器，用于感知道路上的相关信息，且信息内容不能被篡改。

表 1　　**车联网虚假信息检测方法**

方法	基于节点特征的方法		基于信息特征的方法	
	信任机制	投票机制	分类器优化	多源特征
优点	检测简单，开销小	能测出有历史行为的恶意节点	信息特征越多，检测精度越高	信息源越多，检测精度越高
缺点	受恶意节点的信任值影响	受恶意节点比例影响	检测复杂度高	依赖于环境因素
综合分析	检测简单，适用于车联网环境；依赖于通信环境，对消息判断往往不准确		信息特征和信息源越多，检测率越高；检测复杂度较高、警报信息较多时，时延会损害警报信息的时效性	

假设 2：车联网中大部分车辆发送的警报信息是可信的。

3.2 攻击模型

恶意攻击者针对车联网中警报信息的攻击方式主要有散布虚假信息和阻碍信息传播[5,16]。

散布虚假信息是指攻击者通过发布伪造的虚假信息，篡改真实信息，或者注入无效信息改变其他车辆驾驶行为。如当合法车辆收到虚假的前方拥堵的警报信息时，可能会改变行驶路线。

阻碍信息传播是指攻击者抑制、拘留警报信息，甚至发动选择性传递攻击。选择性传递攻击[16]能够结合如虫洞攻击、女巫攻击等一些针对路由发动的攻击，发挥显著的破坏作用。如恶意车辆将通过自身的交通事故警报丢弃，导致后方车辆不能接收到警报通知，使其没有时间做出正确反应，甚至可能导致连环碰撞事件的发生。

本文主要针对散布虚假消息这一攻击方式，采用弱分类器并行检测技术，从分割为多个特征子集的警报信息中检测出虚假信息。

3.3 信息特征定义

在实际交通环境中，车辆行驶安全会受车速、实时路况信息以及突发情况下驾驶员的操作反应等因素的影响[17]。将发送警报信息的车辆节点信息和事件信息相结合，共同作为警报信息的有效特征，有助于对虚假警报的检测。因此，对警报信息分组的有效特征进行扩充，车辆节点向邻居节点广播的信息中包含事件特征信息和车辆自身状态信息。表 2 列出交通警报信息分组中的有效特征，其中，特征名称后面括号中的符号为该特征的简称。

表 2　交通警报信息报文中的有效特征

序号	特征名称
1	Sender (s)
2	Priority (p)
3	Occur time (t_0)
4	Occur site (l_0)
5	Trans time (t_s)
6	Trans site (l_s)
7	Direction (d_s)
8	Vehicle vel (v_s)
9	Vehicle acc (a_s)
10	Reputation (r_s)
11	Retransmit (n)

1) Sender 为发送者的类型。s 为 0 表示警报信息由 RSU 自主发布，认为该信息完全可信，可作为训练数据；s 为 1 表示信息由车辆节点发送。

2) Priority 为交通警报信息的优先级。不同的安全警报事件设置不同的 p 值。如碰撞警告设置为 1、紧急车辆警告设置为 2，p 值越小优先级越高。

3) Occur time 和 Occur site 分别为事件发生的时间 t_0 和地点 l_0。

4) Trans time、Trans site、Vehicle vel 和 Vehicle acc 分别为发送警报信息的时间 t_s、警报信息发送时发送车辆的位置 l_s、速度 v_s 和加速度 a_s。

5) Direction 为车辆发送分组时的行驶方向 d_s。以正北方向为 0 度，通过对比车辆行驶与正北方向的夹角来判断 d_s，一跳两端节点车辆若同向行驶取值 1，反向取值 0。

6) Reputation 为发送车辆的信誉值 r_s，主要根据车辆的历史行为得到。若发现车辆存在攻击行为，则降低 r_s。

7) Retransmit 为警报信息转发的次数 n。某个警报信息的 n 值越大，该警报信息的可信度就越低。设定当 n>10 时，不再转发此警报信息。

3.4 特征分割规则

扩充警报信息的特征在提高虚假信息检测精度的同时，也会增加检测警报信息的算法复杂度，当接收到大量警报信息时，检测警报的时延会破坏警报信息的时效性。因此，本文采取将警报信息中的有效特征分割到不同的集合中，分别同时进行检测，以减少检测时间。

具体做法为：根据警报信息的不同特征设计分割规则，建立事件紧急度、道路状况、信息可信度 3 个特征子集，将耦合度较高的特征归入对应的特征子集中。表 3 为分割后的特征子集和特征对应表。

表 3　警报信息的特征分割

特征子集	子集名称	子集内容
特征子集 1	事件紧急度	t_0, l_0, p
特征子集 2	道路状况	t_s, l_s, v_s, a_s, d_s
特征子集 3	信息可信度	r_s, n

1) 事件紧急度

主要和事件的优先级、事件与接收者之间的距离有关，同时，事件发生时间也作为判断事件紧急度的参考因素。因此，特征子集 1 中包含有 t_0、l_0、p 这 3 个特征。特征 p 有具体的值，而对于特征 t_0、

l_0 由于不同车辆存在事件距离不同，反应时间等特殊因素，使 t_0、l_0 在可接受的范围内有一定的误差。

2) 道路状况

主要与发送警报信息车辆的自身状态信息有关。在特征子集 2 中包含特征 t_s、l_s、v_s、a_s、d_s，该特征子集中的特征维数较多。

3) 信息可信度

主要受发送警报信息的实体信誉值和警报信息转发次数的影响。r_s 与自身的历史行为有关并受其他车辆的评估，n 与警报转发的次数有关。

4　WCIT 方法

WCIT 方法在检测警报信息是否为虚假信息时，主要根据警报信息中发送节点的特征值和事件的特征值（如表 2 所示）进行判断。首先，信息收集模块收集警报信息并分类；其次，预处理模块提取警报信息的特征，并判断待检测信息的有效性和可信性；然后，虚假交通信息检测模块将特征分入不同的特征子集，并输入到各自的弱分类器中进行训练，得出检测结果；最后，如果是有效警报信息，后期处理模块完成预警处理等后续工作。图 2 为基于弱分类器集成的虚假交通信息检测方法框架。

4.1　信息收集

信息收集模块实现信息分类。通过传感器探测，将 RSU 发布的警报作为训练数据，将邻居节点转发的警报信息作为待检测数据。当训练数据由于其他原因不能使用或不足而无法训练时，将随机的待检测信息作为训练补充。警报信息可表示为 I_{is}，表示由节点 s 发送的关于事件 i 的警报信息。信息收集模块对确定事件的真实性具有决定性因素，本文方案假设的场景是高密度交通场景，为此可保证警报的事件拥有充足的来源。信息收集模块流程如图 3 所示。

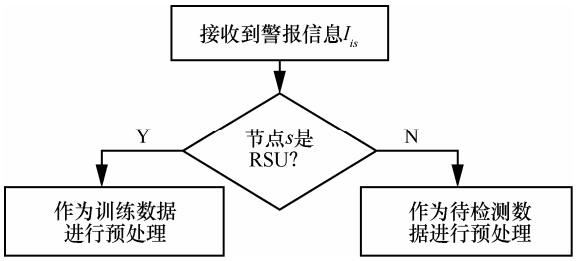


图 3　信息收集模块流程

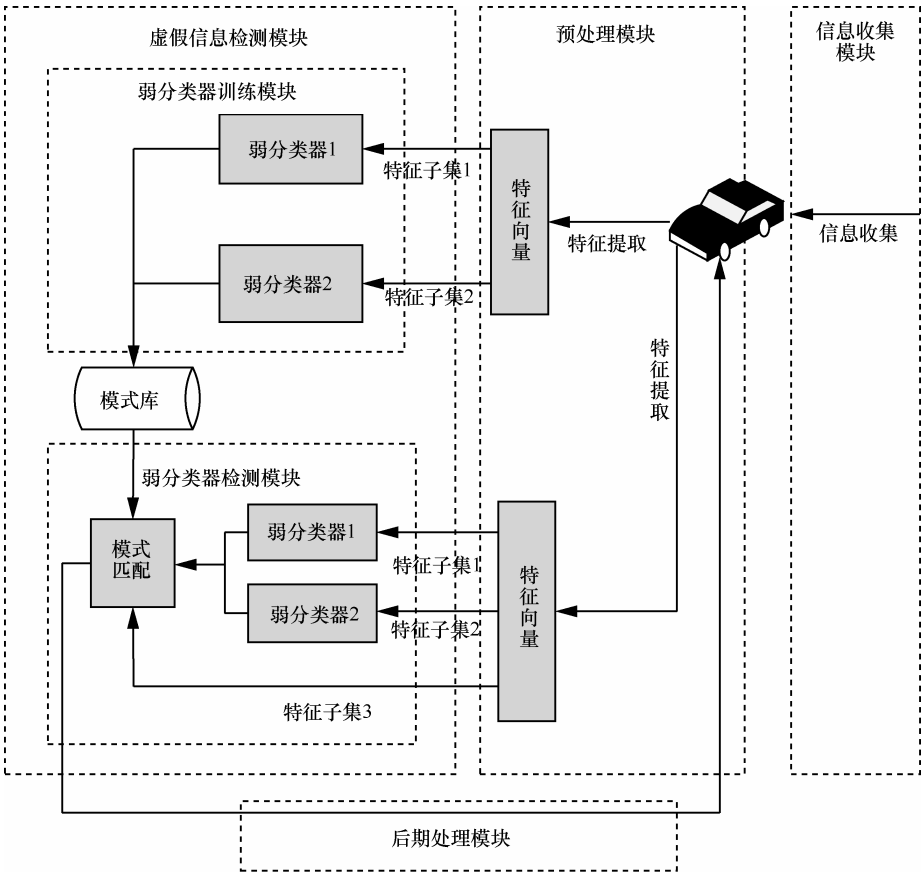


图 2　基于弱分类器集成的虚假信息检测方法框架

4.2　预处理

预处理模块的任务包括警报信息中有效特征的提取、警报信息的有效性检测和信息的可信度判断。

警报信息中有效特征的提取过程表示为

$$F_{is}(k)=f(I_{is}(k)),\ k=1,2,\cdots,n \tag{1}$$

其中，$F_{is}(k)$表示节点 s 发送的关于事件 i 的第 k 个警报信息的有效特征。

为了减少因检测无效警报信息而造成的时间浪费，需要对警报信息的有效性进行判断，将超过时间和空间范围的信息舍弃。警报信息的时间有效性表示为

$$t-t_{\mathrm{s}}<\Delta t \tag{2}$$

其中，t 表示接收警报信息的时间，t_{s} 表示警报信息发送或转发的时间。当式(2)成立时，对该警报信息进行虚假检测，否则直接丢弃该信息。

判断警报信息的空间有效性主要根据事件发生的位置 l_0 是否在接收车辆的前方，如果事件发生在接收车辆的后方，接收车辆不考虑该警报，因为该事件不会对其产生影响。

计算信息的可信度则是作为后期处理模块中判断虚假警报信息的依据。由于车辆接收的警报信息可能经过多跳转发，经过的转发车辆越多，警报的真实性就越低。警报信息的可信度表示为

$$A_i=\mu\frac{r_{\mathrm{s}}}{n_i} \tag{3}$$

其中，μ为可信参数，r_{s}为发送节点 s 的信誉值，n_i为警报信息转发的跳数。

图 4 是待检测警报信息的预处理流程。RSU 发出的警报信息是真实可信的有效信息，作为训练数据进行预处理时，只需完成特征信息的提取。

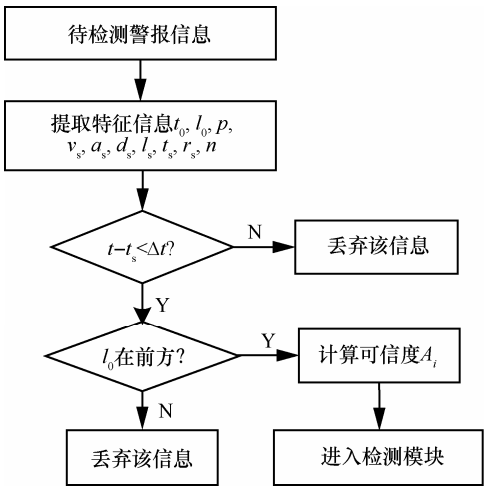


图 4　待检测警报信息预处理流程

4.3　虚假交通信息检测

虚假交通信息检测模块将预处理后的警报信息进行特征分割，将部分特征子集分别输入到对应的弱分类器中，利用学习算法训练得到警报信息的模式(w_1, w_2)并将其存储在模式库中。检测警报信息时，将各子集检测得到的结果集成，再与事件模式进行匹配，并结合信息可信度判断出虚假警报。具体流程如图 5 所示。

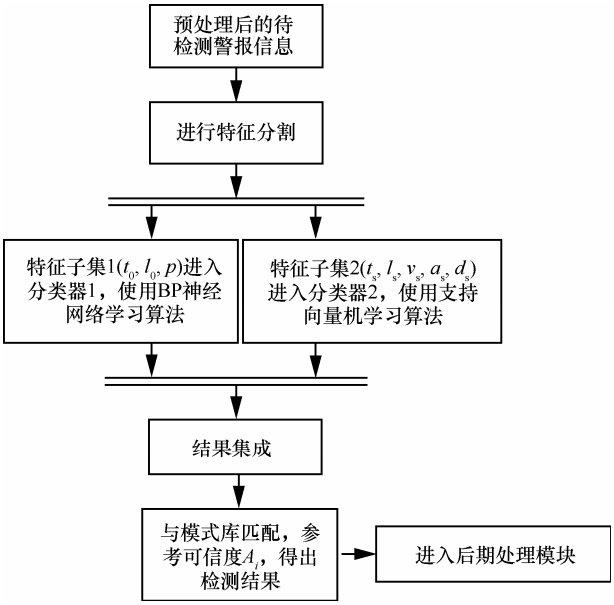


图 5　虚假信息检测模块流程

1) BP 神经网络学习算法

由于 BP 神经网络具有较强的非线性映射能力、高度学习和自适应能力，且具有良好的泛化和一定的容错能力，因此，被用作警报信息的特征子集 1 的分类方法。BP 神经网络权值调整采用反向传播的学习算法，它利用均方误差和梯度下降法来实现对网络连接权值的修正。为了加快收敛速度，防止陷入局部极小值，在此使用动量—自适应学习率调整 BP 算法加快检测速度。动量—自适应学习率 BP 神经网络的权值修正可表示为

$$w(k+1)=w(k)+\alpha(k)(1-\eta)D(k)+\eta D(k) \tag{4}$$

其中，$w(k)$为第 k 步时的权值，$D(k)$为第 k 步时的负梯度，η为动量因子，α为学习率。

2) 支持向量机学习算法

支持向量机（SVM）对非线性和高维数据具有很好的识别能力和良好的泛化能力，因此，被用作对警报信息的特征子集 2 的分类方法。警报信息的特征子集 2 是五维的特征向量，通过 SVM 算法找

到一个最优分类超平面以最大间隔将真实数据与虚假数据分开。

最优分类超平面问题可以表示为

$$\begin{cases}\varphi(w,\xi_i)=\dfrac{1}{2}\|w\|^2+C\sum\limits_{i=1}^{l}\xi_i \\ y_i((wx_i)+b)\geqslant 1-\xi_i\end{cases} \quad i=1,2,\cdots,l \qquad (5)$$

其中，ξ_i 为松弛变量，C 为惩罚因子，w、b 分别为权值和阈值。

4.4　后期处理

后期处理模块需要根据警告信息完成预警处理、转发有效信息和调整车辆信誉值。图 6 是后期处理模块流程。

预警处理是要在接收到有效的警报信息时，立即警告驾驶人，做好安全应急措施。

转发有效信息是指将有效警报信息发送给同向并在本车后方的车辆。

另外，还要根据车辆提供消息的真假，修改相关车辆的信誉值 r_s。如果车辆发送的是真实信息，则增加 r_s，否则减少 r_s，并发送修改后的 r_s 给 RSU，更新本地信誉值列表。

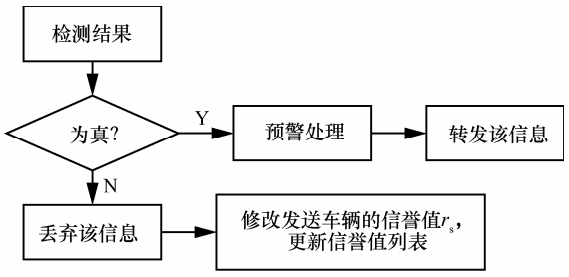


图 6　后期处理模块流程

5　仿真实验与性能分析

本文利用交通仿真软件 VanetMobisim 搭建道路仿真场景，模拟车辆的运动轨迹，获取训练和检测所需的警报信息。在相同情况下，分别使用本文提出的 WCIT 方法和 BPNN 方法[15]对待检测警报信息中的虚假信息进行检测，并比较这 2 种方法在检测开销和检测率方面的性能。此外，从理论上比较并分析 WCIT 方法和多源信息检测过滤方法[14]的通信开销，进而验证本文方法的整体性能。

5.1　仿真环境与参数设置

本文在 VanetMobiSim 中搭建了一个 1 000 m×1 000 m 的二维城市环境，利用 xml 的配置文件进行宏观和微观模型参数的设置，车道设置为常见的双向车道，选择 100 个车辆节点按着道路随机移动，每 0.05 s 对各个节点的位置进行模拟。仿真参数如表 4 所示。

表 4　　交通仿真参数配置

仿真参数	参数值
仿真时间	1 000 s
仿真场景范围	1 000 m×1 000 m
道路数量	Random
车辆数目	100 辆
车辆速度	10~30 m/s
移动录制时间步长	0.05 s

WCIT 方法中根据特征子集 1 检测虚假信息和 BPNN 方法中使用细过滤模块检测虚假信息都采用 BP 神经网络学习算法，对 BP 神经网络的相关设定如下。输入神经元数为 3（如表 3 所示，特征子集 1），输出神经元数为 1（值为 1 或 0，1 表示有效信息，0 表示虚假信息），隐层神经元数为 4，误差精度 0.000 1，激励函数为 $f(x)=\dfrac{1}{1+\mathrm{e}^{-x}}$，训练次数 300 次，输入数据在训练和检测之前都要进行归一化处理。

此外，本文根据特征子集 2 检测虚假信息时，采用 SVM 学习算法。建模前，先对特征子集 2 中的 5 个特征因子做归一化处理，选择最常用的径向基核函数，随机选取训练集中 80%的数据作为建模样本，其余 20%作为检验样本，使用交叉检验的方法确定核参数 g=0.28，惩罚因子 C=100。

在实验中，训练数据分组包括 10 000 条有效信息和 5 000 条虚假信息，检测数据分组包括 3 000 条有效信息和 1 500 条虚假信息。当选取不同数量的警报信息测试检测开销和检测率时，待检测警报信息中有效信息和虚假信息的比例设置约为 2:1。本文方法根据特征子集 1 和特征子集 2 分别检测虚假警报信息时，取两者中检测出的较大的虚假信息数量求检测率。

5.2　结果分析

1) 检测开销

检测开销主要衡量待检测的警报信息进行检测时所需的检测时间。WCIT 方法对警报信息的有效特征进行分割，多个特征子集同时进行虚假检测，故警报信息的检测开销由需要较长检测开销的特征子集决定。WCIT 方法和 BPNN 方法的检测开销对比如图 7 所示。

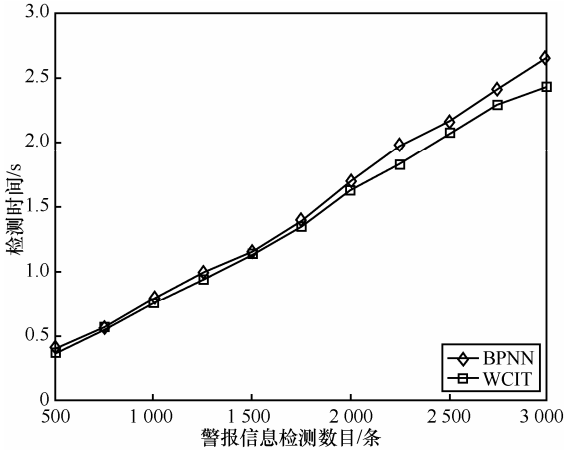


图 7　BPNN 与本文方法的检测开销对比

从图 7 中可以看出，当检测的警报信息数量不太多时，2 种方法所需的检测开销差别不大。随着需要检测的警报信息数量的增加，BPNN 方法所需的检测时间逐渐变长，超过 WCIT 方法，时间开销相比本文方法有越来越大的趋势。这和 BPNN 方法采用 2 次过滤的方式有关。

2) 检测率

检测率是指检测系统能够正确检测出虚假警报信息的概率。检测率越高，说明检测方法的性能越好。

如图 8 所示，随着检测的警报信息数目的增加，检测率的值呈下降趋势。由于使用了综合特征，WCIT 方法的检测率优于仅使用部分特征的 BPNN 方法。WCIT 方法可以在高密度场景中快速地检测出虚假警报且能够保证较高的检测率。

3) 通信开销

本文设置新型分组（如表 2 所示）为警报信息提供足够的信息特征。Kim 等[14]则采用多源信息检测过滤方法，每个信息源发送的分组中，警报信息仅包含表 2 中的部分信息特征，要获取所有信息特征，需接收多个信息源发送的事件消息。

表 5 举例说明本文和文献[14]的警报信息分组的发送情况。其中，警报数据由表 2 中的信息特征组成。假定警报数据中每个信息特征所占字节固定，√ 表示节点发送的分组中包含这项特征。节点 1 发送本文设置的新型分组，一次性发送的分组包含了所有信息特征。节点 2 和节点 3 作为文献[14]中的 2 种信息源发送分组，每个分组包含部分信息特征。由表 5 可知，本文方法在一次分组发送中包含的信息特征在文献[14]方法中需要通过 2 次甚至多次分组发送才可获得，由于每个信息源发送的分组中存在冗余特征，因而造成通信冗余。当需要检测大量的警报信息时，和文献[14]方法相比，本文方法减少了基于节点识别的通信次数，降低了检测的整体通信代价。

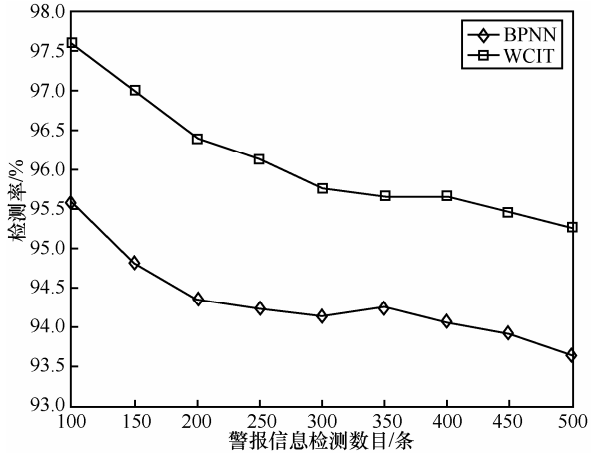


图 8　BPNN 与本文方法的检测率对比

6　结束语

本文针对车联网中需要快速检测大量交通警报信息提高交通安全的问题，提出了一种基于弱分类器集成的虚假交通信息检测方法。该方法扩充了消息分组的有效特征，并设计分割规则将警报信息的综合特征划分为多个特征子集；然后，使用适合的弱分类器分别处理；最后，将分类结果集成来判断警报信息的真实性。实验结果表明，使用弱分类器集成技术降低了检测时间，且由于综合特征的应用，使本文方案的检测率高于使用部分特征的检测方案。下一步工作，考虑在警报信息中设置更多事件周边的基础安全信息，如发送信息车辆的速度、加速度、方向及车辆上安装的各种传感器的感知信

表 5　警报信息分组发送情况

分组内容		警报数据											其他数据
		s	p	v_s	a_s	t_s	l_s	r_s	t_0	l_0	d_s	n	
本文	节点 1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
文献[14]	节点 2	✓	✓					✓	✓	✓		✓	✓
	节点 3	✓	✓	✓	✓	✓	✓				✓		✓

息，通过对这些人为不可更改的特征信息的分析来判定事件的真实性（如震动传感器感知车辆附近是否具有震动，从而判定是否有事故发生等），从而减少目前检测方法中依靠大量外部数据（如 RSU 发送的信息，邻居车辆发送的信息）来检测信息的真实性而带来的时间花费和对数据量的依赖性。

参考文献：

[1] BAIOCCHI A, CUOMO F, FELICE D M, et al. Vehicular ad-hoc networks sampling protocols for traffic monitoring and incident detection in intelligent transportation systems[J]. Transportation Research Part C: Emerging Technologies, 2015, 56: 177-194.

[2] 常促宇, 向勇, 史美林. 车载自组网的现状与发展[J]. 通信学报, 2007, 28(11): 116-126.
CHANG C Y, XIANG Y, SHI M L. Present situation and development of vehicular ad hoc networks[J]. Journal on Communication, 2007, 28(11):116-126.

[3] ABUELELA M. A framework for incident detection and notification in vehicular ad-hoc networks[J]. Dissertations & Theses-Gradworks, 2011.

[4] GROVER J, LAXMI V, GAUR M S. Attack models and infrastructure supported detection mechanisms for position forging attacks in vehicular ad hoc networks[J]. CSI Transactions on Ict, 2013, 1(3): 261-279.

[5] RICHARD G E, MARTINE B, SAMUEL P, et al. VANET security surveys[J]. Computer Communications, 2014, 44:1-13.

[6] GROVER J, PRAJAPATI N K, LAXMI V, et al. Machine learning approach for multiple misbehavior detection in VANET[M]. Advances in Computing and Communications. Berlin Heidelberg: Springer, 2011:644-653.

[7] ZHU W T, ZHOU J, DENG R H, et al. Detecting node replication attacks in wireless sensor networks: a survey[J]. Journal of Network and Computer Applications, 2012, 35(3): 1022-1034.

[8] ABDELAZIZ K C, LAGRAA N, LAKAS A. Trust model with delayed verification for message relay in VANETs[C]//The 2014 International Conference on Wireless Communications and Mobile Computing(IWCMC'14). c2014: 700-705.

[9] DING Q, LI X, JIANG M et al. Reputation-based trust model in vehicular ad hoc networks[C]//The 2010 International Conference on Wireless Communications and Signal Processing (WCSP'14), Suzhou. c2010: 1 - 6.

[10] ZHANG J, CHEN C, COHEN R. Trust modeling for message relay control and local action decision making in VANETs[J]. Security & Communication Networks, 2013, 6(6):1-14.

[11] SHAIKH R A, ALZAHRANI A S. Intrusion-aware trust model for vehicular ad hoc networks[J]. Security & Communication Networks, 2014, 7(11):1652–1669.

[12] OSTERMAIER B, DOTZER F, STRASSBERGER M. Enhancing the security of local danger warnings in VANETs-a simulative analysis of voting schemes[C]//The 2nd International Conference on Availability, Reliability and Security. c2007:422-431.

[13] 李春彦, 刘怡良, 王良民. 车载自组网中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.

[14] KIM T H J, STUDER A, DUBEY R, et al. VANET alert endorsement using multi-source filters[C]//The 7th ACM International Workshop on Vehicular Ad Hoc Networks. c2010:51-60.

[15] ZHANG J Y, HUANG L X, XU M J, et al. An incremental BP neural network based spurious message filter for VANET[C]//The 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery(CyberC'12). Sanya, c2012: 360-367.

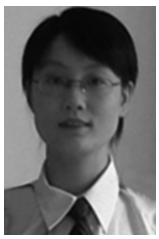
[16] LIM S, HUIE L. Hop-by-hop cooperative detection of selective forwarding attacks in energy harvesting wireless sensor networks[C]//The 2015 IEEE International Conference on Computing, Networking and Communications (ICNC'2015). c2015: 315-319.

[17] 詹珂昕. 高速公路 VANET 预警信息传播机制的研究[D]. 北京: 北京交通大学, 2012.
ZHAN K X. Propagation mechanism of highway safety warning message based on VANET[D]. Beijing: Beijing Jiaotong University, 2012.

作者简介：

刘湘雯（1979-），女，江苏宜兴人，江苏大学讲师，主要研究方向为车联网与大数据安全、隐私保护。

石亚丽（1992-），女，安徽芜湖人，江苏大学硕士生，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。