文章编号：2095-2163(2021)12-0054-07 中图分类号：TP391 文献标志码：A

VANET 中 Sybil 攻击检测系统的研究

齐健翔[1]，李文博[2]，岳克强[3]
（1 新乡学院 计算机与信息工程学院，河南 新乡 453003；2 新乡学院 化学与材料工程学院，河南 新乡 453003；
3 杭州电子科技大学 电子信息学院，杭州 310018）

摘 要：由于车辆的高速移动性、网络拓扑的动态变化性以及无线信道的脆弱性和开放性，车载自组织网络面临着多种安全威胁，女巫攻击便是其中的一个典型代表。攻击者通过盗用或伪造多个不同身份，发布各种虚假信息，影响网络中的节点决策机制、资源分配机制以及路由转发机制。为了解决这个安全隐患，本文设计一种女巫攻击检测系统，利用层次聚类和动态邻域检测的方法，分析车辆行驶数据的空间关联性和时间相似性，从而识别出网络中存在的攻击节点。实验表明，该系统具有较高的检测率，较强的环境适应性、抗攻击性和鲁棒性。

关键词：车载自组织网络；女巫攻击；层次聚类；动态邻域检测

Research on the detection system of Sybil attack in VANET

QI Jianxiang[1], LI Wenbo[2], YUE Keqiang[3]
(1 School of Computer and Information Engineering, Xinxiang University, Xinxiang Henan 453003, China;
2 School of Chemical and Material Engineering, Xinxiang University, Xinxiang Henan 453003, China;
3 School of Electronic Information, Hangzhou Dianzi University, Hangzhou 310018, China)

【Abstract】VANET is faced various security threats due to the high-speed mobility of vehicles, the dynamic change of network topology, and the vulnerability and openness of wireless channels. The Sybil attack is a typical representative. The attacker releases various false information by stealing or forging several different identities to affect the node decision mechanism, resource allocation mechanism and routing and forwarding mechanism in the network. In order to address this security risk, a detection system of Sybil attack based on the methods of hierarchical clustering and dynamic neighborhood detection is designed. The attacking nodes present in the network are identified by analyzing the spatial correlation and temporal similarity of vehicles' travelling data. The experiments show that the system has a high detection rate, strong environmental adaptability resistance of attack and robustness.

【Key words】VANET; Sybil attack; hierarchical clustering; dynamic neighborhood detection

0 引 言

作为移动自组织网络(MANET)在交通领域的典型应用，车载自组织网络(VANET)近年来得到了快速的发展和推广[1]。道路上行驶的车辆之间、车辆与路侧基础设施之间通过建立自组织网络，利用 V2V 和 V2I 的方式实现数据的有效传输和共享，使得车辆能够获取“视野”之外的交通信息，扩展了车辆的感知范围，从而很大程度上提高了用户的出行安全和通行效率。车辆节点之间数据传输的稳定性、有效性以及真实性是 VANET 的基本需求，也是车联网相关衍生服务必不可缺的一个重要组成部分[2]。然而，由于车辆的高速移动性和行驶路线的随机性，导致 VANET 的网络拓扑具有较大的动态性，车辆之间的通信链路极不稳定，而且面临着不断地中断与重连，再加上无线通信固有的脆弱性和开放性，使得车联网通信面临着严重的安全威胁[3]。目前，VANET 中常见的攻击行为主要包括：虚假信息攻击、拒绝服务攻击、伪装攻击、黑洞攻击、时序攻击、位置欺骗攻击、中间人攻击和 Sybil 攻击等[4-5]。其中，Sybil 攻击是其中的一个典型代表。

1 相关工作

Sybil 攻击也被称为女巫攻击，最初是由 Decour 在 P2P 网络中提出，属于一种基于身份混淆的攻击方式[6]。攻击者通过盗用、伪造等手段获取多个不同的身份，通过利用这些身份发布各种虚假信息，从而影响网络中的节点决策机制、资源分配机制以及

基金项目：浙江省重点研发计划项目(2019C01070)。

作者简介：齐健翔(1983-)，男，硕士，助教，主要研究方向：物联网技术应用、物联网安全；李文博(1986-)，女，博士，讲师，主要研究方向：新能源汽车动力电源技术；岳克强(1984-)，男，博士，讲师，主要研究方向：无线自组网应用、移动计算、信息物理系统安全。
通讯作者：齐健翔 Email：qjx1011@126.com

收稿日期：2021-10-18

路由转发机制等[7]。例如，在社交网络中通过雇佣大量“水军”来提高特定节点的影响力；在出租车运营网络中通过注册多个不同身份来提高获取订单的成功率；在 VANET 中通过多个伪造身份同时发布虚假的路况信息，造成交通拥堵。

VANET 中针对 Sybil 攻击的检测方案大致分为以下 4 种，如图 1 所示[8]。

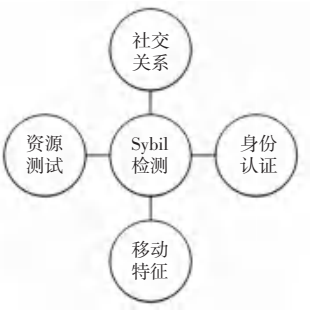

图 1　Sybil 攻击的检测方案分类

Fig. 1　Classification of detection schemes for Sybil attacks

(1)基于社交关系的检测方案。该方法根据节点之间的交互情况，建立相应的社交关系来检测网络中是否存在 Sybil 攻击行为[9]。为了提高在网络中的影响力和话语权，Sybil 节点通常会与其他虚假节点进行频繁交互，快速提升其在网络中的声望，最终达到影响和干预其他节点作出相关决策的目的[10]；而虚假节点与其他真实存在的正常节点之间的交互则非常有限。针对这种攻击方式，通过分析网络中节点之间的社交行为特征，从而检测出具有 Sybil 攻击嫌疑的对象。

尽管该检测方法在社交网络领域非常有效，但是在 VANET 中，由于车辆的高速移动性和路线随机性，车辆之间无法保持较长时间的有效交互，车与车之间难以建立稳定的社交关系，因此，基于社交关系的检测方法不适用于 VANET 中的 Sybil 攻击检测。

(2)基于资源测试的检测方案。与路侧单元(Road Side Unit，RSU)和充当后台服务器的可信机构(Trust Authority，TA)相比，车载单元在通信资源、计算资源以及存储资源等方面都极其有限，正常情况下，仅依靠单个节点无法在指定时间内完成多个节点的任务总和[11-12]。因此，利用资源测试的方式，通过对比节点的工作完成度，能够有效地识别出网络中的 Sybil 攻击节点。

尽管基于资源测试的检测方法简单易行，但是随着软、硬件技术的发展，车载设备的性能大幅度地提升，当攻击节点拥有足够多的资源时，该方法针对 Sybil 攻击的检测效率会急剧下降。

(3)基于身份认证的检测方案。在移动通信网络中，为了保证通信节点的身份合法性，通信内容的机密性和不可否认性，后台管理中心通过引入 PKI 技术，利用密钥管理及数字签名等手段，验证通信节点的身份合法性，从而实现对于 Sybil 攻击节点虚构的其他身份进行有效甄别[13-14]。例如，通过使用群签名等方法，能够有效的抑制 Sybil 节点伪装成多个不同身份，散布虚假信息[15]。

基于身份认证的检测方法从理论方面来讲是切实有效的，但是当攻击节点通过盗用其他合法节点的身份信息，或者多个攻击者之间存在合谋时，可以轻易逃避该方法的检测。

(4)基于移动特征的检测方案。节点的高速移动性是 VANET 的一个重要特征。一般情况下，由于车辆的路线随机性，车与车之间无法长期保持相似的移动特性[16]。尽管 Sybil 攻击节点能够伪造出多个不同的身份与外界进行交互，由于这些虚假身份都映射到同一个物理节点，因此，攻击节点及其“分身”的移动行为具有一定的相似性。通过对节点移动行为进行时序性分析，从而判断其是否存在 Sybil 攻击的嫌疑[17]。

由于对车辆移动行为分析的过程受时间粒度的影响较大，由此形成的粗粒度的轨迹数据无法准确、全面的反映车辆的移动行为特征，从而对相似性分析结果产生较大的干扰；另外，攻击节点也会采用位置扰动技术或者功率控制技术，降低伪造身份之间的行为相似性和位置相似性，从而逃避相关的检测方案。

2　研究内容

2.1　系统模型

本文提出的 Sybil 攻击检测系统模型如图 2 所示，主要包括车辆(Vehicles)、路侧单元(Road Side Unit，RSU)和可信机构(Trust Authority，TA)3 个部分，其具体特点如下：

(1)车辆。车辆上安装有多种传感设备，能够实时获取车辆的各项行驶参数，主要包括：速度、加速度、行驶方向等；同时，车辆通过配备定位装置，例如：北斗定位系统，可以实时获取车辆当前所在的位置信息；通过配备无线电通信装置，实现车辆之间以及车辆与 RSU 之间的数据传输和共享。

(2)路侧单元 RSU。路侧单元有时也被称为基

站,通常被视为连接车辆和可信机构的桥梁,是维系整个检测系统有效运行的重要枢纽。一方面,路侧单元可以对有效通信范围内的车辆进行统一管理,收集现场的交通数据和车辆信息并上传至可信机构;另一方面,路侧单元接收可信机构下发的管理命令,并将信息传输至特定的车辆。路侧单元与车辆之间采用专用短程通信技术(Dedicated Short Range Communications, DSRC)进行无线通信;路侧单元之间以及路侧单元与可信机构之间则采用光缆进行有线通信。

(3)可信机构。在本文研究的 Sybil 攻击检测系统中,默认可信机构是绝对安全的,完全可以抵抗恶意攻击者的入侵和数据篡改。可信机构的主要职责包括:

①车辆身份证书管理。车辆出厂后首先会在可信机构进行身份注册,获取合法身份后方可上路。当车辆被确认存在恶意攻击行为后,可信机构将注销其身份证书,使之无法继续参与 VANET 的正常活动。

②数据存储和计算。与极其有限的车载资源相比,可信机构拥有强大的计算能力和充足的存储空间。路侧单元定期将其通信范围内的车辆信息上传至可信机构,由可信机构对这些信息进行分析处理,提取有效的车辆轨迹信息和动态邻域信息,最终利用相关的检测模型对 VANET 中存在的恶意攻击行为进行有效甄别。

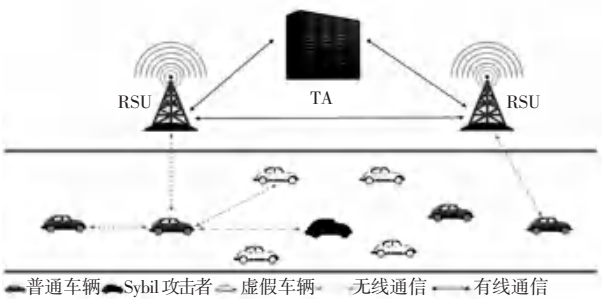

图 2 Sybil 攻击检测系统模型

Fig. 2 Detection system model of Sybil attack

2.2 攻击模型

攻击者通过盗用或窃取等不当手段生成包含 n 个伪造身份的假名集合 $\{PID_1,\cdots,PID_n\}$,利用这些假名信息构造出多个虚假车辆,进而发动 Sybil 攻击。根据攻击者采取的不同行为模式,可将其大致分为两类:

(1)固定位置攻击。攻击者利用假名集合构建出若干虚假车辆,这些伪造车辆与周围其他车辆和距离其最近的 RSU 进行数据通信时,传输信息中包含的位置数据均为攻击者的真实位置坐标,没有经过任何修改。

(2)随机位置攻击。攻击者在其真实位置信息的基础上,利用信息扰动技术生成多组随机位置坐标。当攻击者发动 Sybil 攻击时,伪造的车辆使用不同的位置坐标与外界进行数据交互,其目的在于降低攻击者与虚假车辆之间行驶轨迹的相似程度,从而避免其攻击行为被检测系统识别。

2.3 检测方案

2.3.1 准备工作

车辆只有在注册并获取到有效的身份证书后方可加入 VANET 上路行驶。在行驶过程中,车辆需要向最近的 RSU 申请临时通行凭证。该凭证具有一定的时效性,在有效期内车辆可以及时与外界进行数据通信,获取所需的服务信息;超出规定的时间后,该凭证自动失效,车辆需要再次向 RSU 提出申请,否则将无法继续与 VANET 中的其他车辆进行信息交互。此外,车辆在正常参与 VANET 相关活动过程中,需要周期性地广播 Beacon 消息,向周边相邻车辆提供自己的行驶状态,例如:速度、加速度、方向盘转角、刹车状态、位置信息等。对于接收到 Beacon 消息,车辆根据通信数据与临时凭证的对应关系建立相应的邻域信息,并在本地进行存储,等到下次向 RSU 申请新的临时凭证时,将该时间段内收集的所有邻域信息经由 RSU 上传至 TA,以便后期进行数据分析和攻击行为检测。

2.3.2 轨迹相似性检测

TA 将一段时间内各个 RSU 上传的数据信息按时序进行重组和整合,可以获取在此期间所有车辆(包括物理世界真实存在的车辆以及由攻击者“制造”出来的虚假车辆)的行驶轨迹。车辆的行驶轨迹包含若干不同的轨迹点数据,而每个轨迹点数据则是由对应的经纬度信息及时间戳所组成,即:$TRACK_i = \{P_{i1}, P_{i2},\cdots,P_{in}\}$,且 $P_{ij} = \{lo_{ij}, la_{ij}, T_{ij}\}$。对于任意两辆车 m 和 n 上传的轨迹数据,根据时间关联性建立包含 k 个轨迹“点对”的集合 $PS_{mn} = \{\{P_{m1}P_{n1}\}, \{P_{m2}P_{n2}\}, \cdots, \{P_{mk}P_{nk}\}\}$,如图 3 所示。集合中的每一对轨迹点分别隶属于不同的车辆,并且二者具有相似的时域信息,即二者的时间戳差值应当不超过预设的阈值 $TIME_{threshold}$。通过分析各个轨迹点对之间的特征相似性,利用数据挖掘的方法找出发动 Sybil 攻击的车辆及其虚构的各个“分身”。

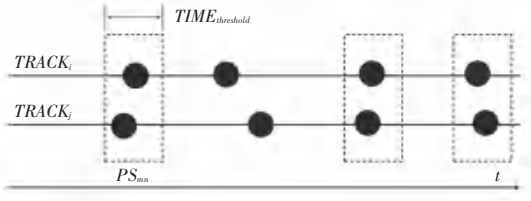

图 3　轨迹点对集合

Fig. 3　Set of track point pairs

2.3.2.1　原始轨迹数据清洗

尽管可信机构 TA 具有非常强大的数据存储和处理能力，但是面对海量的汽车轨迹数据以及无线自组织网络中难以避免产生的冗余信息，直接对其进行无差别处理将会给 TA 服务器造成巨大的负荷。因此，在进行车辆轨迹相似性检测之前，对这些海量数据采取相应的预处理是非常有必要的。本文主要从空间差异和时间差异相结合的角度出发，过滤掉那些完全不可能由同一辆车产生的轨迹信息，减小数据量过大给服务器带来的压力。

通过对轨迹点对集合 PS_{mn} 进行遍历，一旦发现其中任意一对轨迹点 $\{P_{mk}P_{nk}\}$ 满足关系(1)，则该集合对应的轨迹信息应当隶属于两个不同的车辆，不存在 Sybil 攻击的嫌疑。

$$\sqrt{(lo_{mk}-lo_{nk})^2+(la_{mk}-la_{nk})^2} > |T_{mk}-T_{nk}| * \mathrm{Max}(V_{mk}, V_{nk}) \quad (1)$$

其中，V_{mk} 和 V_{nk} 为车辆上传的 Beacon 信息中与该时间戳对应的速度信息。

由关系式(1)可知，即使车辆在当前时刻以最大速度行驶，仍然无法在有效时间内经过点对中的两个位置，该轨迹点对不可能来自同一辆车，可以将这两条轨迹数据从待检测数据集中删除。

2.3.2.2　基于层次聚类的轨迹相似性检测

对原始轨迹数据进行过滤，排除掉那些属于正常车辆的轨迹信息，剩余部分均为具有 Sybil 攻击嫌疑的车辆轨迹。针对这部分数据，首先根据车辆轨迹相似性的检测原理建立对应的特征模型，主要包括：空间差异 SD_{mn}^{space}，时间差异 SD_{mn}^{time}，速度差异 SD_{mn}^{speed} 以及航向差异 $SD_{mn}^{heading}$；利用数据挖掘技术进行聚类处理，根据聚类结果最终判断轨迹信息的相似性，式(2) ~ (5)。

$$SD_{mn}^{space}=\sqrt{(lo_{mk}-lo_{nk})^2+(la_{mk}-la_{nk})^2} \quad (2)$$

$$SD_{mn}^{time}=|T_{mk}-T_{nk}| \quad (3)$$

$$SD_{mn}^{speed}=|V_{mk}-V_{nk}| \quad (4)$$

$$SD_{mn}^{heading}=\begin{cases}-1, & \text{车辆 } m \text{ 和车辆 } n \text{ 反向}\\ 1, & \text{车辆 } m \text{ 和车辆 } n \text{ 同向}\\ 0, & \text{其他}\end{cases} \quad (5)$$

聚类算法在许多研究领域和工程实践中得到了广泛应用，根据其理论依据和应用模式不同，主要分为划分法、层次法、密度法、图论聚类法、网格法、模型法等。鉴于轨迹点对数据的结构特点及聚类结果的不确定性，本文采用层次聚类算法，从上述 4 个特征维度对轨迹点对进行聚类处理，具体流程如图 4 所示。

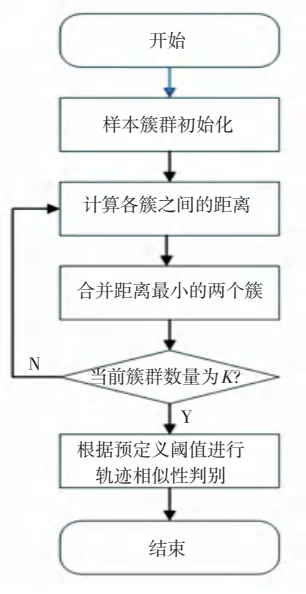

图 4　层次聚类流程图

Fig. 4　Flow chart of hierarchical clustering

2.3.3　动态邻域检测

对于 VANET 中存在的那些采用固定位置攻击的行为，利用前文提出的基于层次聚类的车辆轨迹相似度检测方法，能够准确、有效地辨识出恶意攻击节点及其衍生的若干虚假“分身”。然而，当恶意攻击者通过北斗、GPS 等定位系统获取到有效的位置坐标后，通过采用添加随机扰动数据的手段，生成多个不同的位置信息，在发动 Sybil 攻击时使用不同的位置数据与外界进行交互，可以逃避轨迹相似性检测。

在 VANET 中，车辆通常会以广播的方式与周围其他车辆进行数据传输和共享。在这种交互模式下，接收车辆以时间序列为参考，统计近期向其发送数据的邻居节点，形成对应的邻域信息表，并上传至附近的 RSU。由于无线通信技术的固有特点，车辆之间的相邻性取决于二者之间的实际地理位置及信号发射功率。在上述两个条件均保持不变的情况下，即使恶意节点通过位置伪造来发动 Sybil 攻击，攻击节点及其虚构出来的车辆均会被有效通信范围

内的相邻车辆所捕获,并记录在各自的邻域信息表中。鉴于车辆的高速移动性和路线随机性,车辆之间的相邻关系应该是非常短暂的,无法长期保持同步行驶。因此,通过对不同车辆在一定时间内上传的邻域信息进行分析,如果发现若干车辆频繁出现在不同车辆记录的邻域信息表中,那么这些车辆可能存在发动 Sybil 攻击。当类似情况超出预设的阈值后,可信机构 TA 就会剥夺这些车辆的合法身份,从而阻断其攻击行为给网络带来的安全危害。车辆之间的邻域关系如图 5 和表 1 所示。

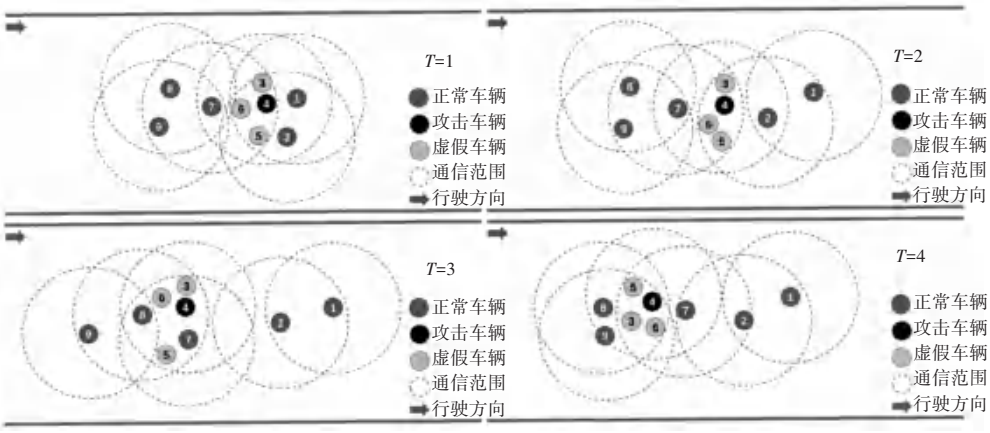

图 5 车辆邻域关系图

Fig. 5 Relationship map of vehicular neighborhood

表 1 车辆邻域结构表

Tab. 1 Structure table of vehicular neighborhood

	$T=1$	$T=2$	$T=3$	$T=4$
V1	V2, V3,V4,V5,V6	V2	V2	V2
V2	V1,V3,V4,V5,V6	V1,V3,V4,V5,V6	V1	V1,V7
V4	V1,V2,V7	V2,V7	V7,V8	V7,V8,V9
V7	V3,V4,V5,V6,V8,V9	V3,V4,V5,V6,V8,V9	V3,V4,V5,V6,V8	V2,V3,V4,V5,V6
V8	V7,V9	V7,V9	V3,V4,V5,V6,V7,V9	V3,V4,V5,V6,V9
V9	V7,V8	V7,V8	V8	V3,V4,V5,V6,V8

动态邻域检测的具体步骤如下:

Step 1 建立各个节点在 T 时刻的邻域信息表 N_i^T;

Step 2 遍历各个节点,统计该节点与其相邻节点之间的邻域信息交集 S_i^T;

Step 3 $S_i^T = S_i^{T-1} \cap S_i^T$, 若 $S_i^T \neq \emptyset$,则计数器 $Clunt_i$ 加 1;

Step 4 若 $Count_i > Count_{threshold}$,且 $S_i^T \neq \emptyset$,则 S_i^T 为 Sybil 攻击者集合;

Step 5 令 $T = T + 1$, 重复执行 Step 1~4。

3 实验仿真

本文实验仿真的核心目标主要包括:

(1)基于层次聚类的车辆轨迹相似性检测算法的有效性和可行性;

(2)在不同的实验条件下,该检测系统应具有较强的适应性、抗攻击性和鲁棒性。

在实验过程中使用 Veins 仿真平台来模拟车辆在道路上的正常数据交互及恶意车辆发动 Sybil 攻击的行为。Veins 是一个广泛应用于车联网模拟仿真的开源框架,内部包含有两个独立的模拟器:SUMO 和 OMNET++。SUMO 主要用于交通仿真,能够模拟不同的交通模式及车辆的移动行为特性,模拟过程中使用的路网信息可以由开源网站 OpenStreetMap 导入指定地理范围内的真实地图数据,也可以使用 XML 文件进行自定义路网设计。OMNET++主要用于网络通信仿真,能够模拟车辆之间以及车辆与 RSU 之间的数据传输过程。SUMO 和 OMNET++之间利用 VEINS 框架提供的"交通控制接口(TraCI)"实现交通数据与通信数据的分布式传输和共享。

本文在仿真过程中使用了新乡市东区的部分路网数据如图 6 所示,具体的实验仿真参数见表 2。

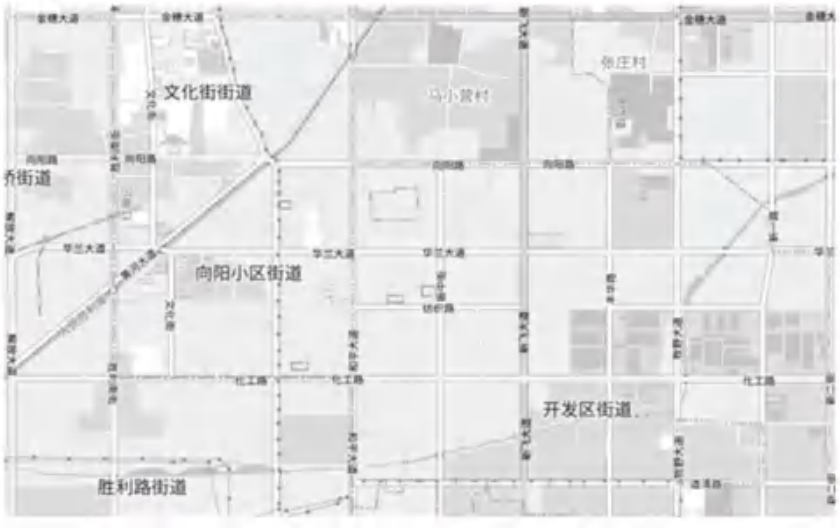

图 6　新乡市东区路网信息

Fig. 6　Road network information about the Eastern District of Xinxiang

表 2　仿真参数

Tab. 2　Simulation parameters

参数	值
仿真区域	5 000×3 000 m
汽车数量	200 辆
通信范围	500 m
攻击者数量	10 辆
车速	0~70 km/h
仿真时间	1 200 s

在 Sybil 攻击检测系统的研究工作中，检测率是本文关注的重点性能指标，其直接关系到该系统是否能够有效地识别出 VANET 中存在的攻击节点。在实验过程中，通过分析 Sybil 检测系统的工作原理与实现过程，本文主要考虑了以下 3 个方面的因素对检测结果的影响：

(1)车辆的行驶速度。在不同的行驶区域(城区和郊区)与不同的时段(平峰期和高峰期)，车辆的行驶速度存在着较大的差异。由于车辆在行驶过程中需要以固定的周期向周边其他车辆广播 Beacon 信息，以及向距离最近的 RSU 申请临时身份并上传邻域信息，而车辆速度的变化将导致车辆轨迹的粒度变化，以及邻域信息的组成结构变化。此外，速度的提高也会加剧车与车之间通信链路的不断中断和重连，导致数据传输的不稳定性和滞后性。因此，随着车辆速度的不断提高，系统的检测率将受其影响而不断降低，如图 7 所示。

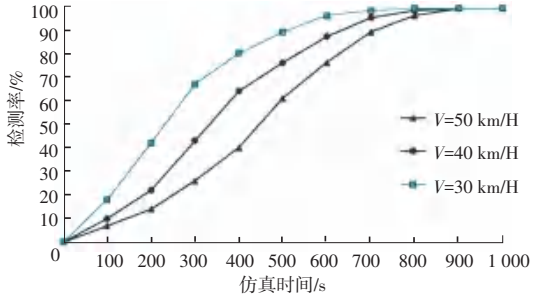

图 7　车速对检测率的影响

Fig. 7　Effect of vehicle's speed on detection rate

(2)通信过程中的丢包率。在 VANET 中，车与车之间(V2V)以及车与 RSU 之间(V2I)的数据共享与传输均采用基于 DSRC 的无线通信方式，通信过程中可能会受到外界各种因素的干扰，导致数据包的丢失。丢包率的高低直接关系到信息采集的完整性和数据来源的有效性，对后期的数据挖掘和信息建模将会产生重大影响，VANET 丢包率的不断增高将导致该系统的检测率不断下降，如图 8 所示。

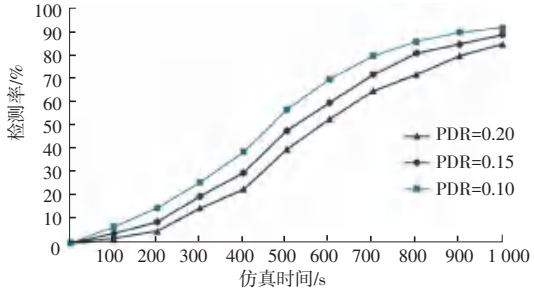

图 8　丢包率对检测率的影响

Fig. 8　Effect of PDR on detection rate

(3)恶意节点的攻击强度。VANET 中恶意节点的攻击强度主要体现在发动 Sybil 攻击的节点数量、攻击者使用的虚假身份数量以及攻击频率。如果恶意节点中仅有部分成员发动攻击,并且使用的虚假身份数量较少,攻击频率较低,系统由于无法收集到足够的"证据"而导致检测效率较低。随着恶意节点的攻击强度不断增大,系统采集到的数据信息中包含的攻击特征,即轨迹数据的空间关联性和邻域信息的时间相似性也会越来越明显。因此,随着恶意节点攻击强度的不断提高,系统的检测率将随之不断上升,如图 9 所示。

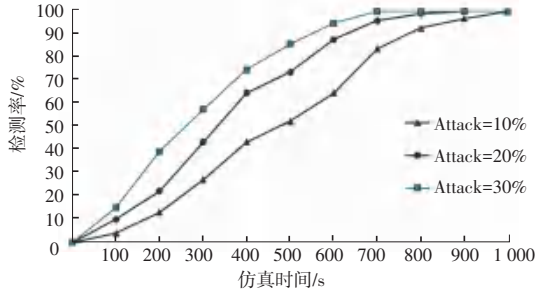

图 9 攻击强度对检测率的影响

Fig. 9 Effect of attack strength on detection rate

4 结束语

本文针对 VANET 中恶意车辆在发动攻击时的行为特征,设计了一种有效的 Sybil 攻击检测系统。该系统利用数据挖掘技术对于车辆行驶轨迹的空间关联性及其邻域信息的相似性展开动态分析,不仅能够适用于检测群组固定位置攻击,对于那些为了逃避检测而添加了信息扰动的随机群组位置攻击也能够很好的识别。实验结果表明,本文设计的 Sybil 攻击检测系统具有较高的检测率,能够有效地识别出 VANET 中存在的恶意攻击者,为网络的正常有效运行提供了保障。在不同的工作环境下,系统的检测效果始终能够保持在一个较高的水准,具有较强的环境适应性和鲁棒性。

参考文献

[1] VASUDEVA A, SOOD M. Survey on sybil attack defense mechanisms in wireless ad hoc networks[J]. Journal of Network and Computer Applications, 2018, 120: 78-118.

[2] GROVER J, GAUR M S, LAXMI V. Multivariate verification for sybil attack detection in VANET[J]. Open Computer Science, 2015, 5(1): 60-78.

[3] CHAUBEY N K, YADAV D. A taxonomy of Sybil attacks in vehicular ad - hoc network (VANET)[M] IoT and Cloud Computing Advancements in Vehicular Ad - Hoc Networks. IGI Global, 2020: 174-190.

[4] AL-MUTAZ M, MALOTT L, CHELLAPPAN S. Detecting Sybil attacks in vehicular networks[J]. Journal of Trust Management, 2014, 1(1): 1-19.

[5] CHANG S, QI Y, ZHU H, et al. Footprint: detecting Sybil attacks in urban vehicular networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 23(6): 1103-1114.

[6] DOUCEUR J R. The sybil attack[C]//International workshop on peer-to-peer systems. Springer, Berlin, Heidelberg, 2002: 251-260.

[7] KUMAR KARN C, PRAKASH GUPTA C. A survey on VANETs security attacks and sybil attack detection[J]. International Journal of Sensors Wireless Communications and Control, 2016, 6(1): 45-62.

[8] YANG Z, ZHANG K, LEI L, et al. A novel classifier exploiting mobility behaviors for sybil detection in connected vehicle systems [J]. IEEE Internet of Things Journal, 2018, 6(2): 2626-2636.

[9] YU H, KAMINSKY M, GIBBONS P B, et al. Sybilguard: defending against sybil attacks via social networks[J]. IEEE/ACM Transactions on networking, 2008, 16(3): 576-589.

[10] MOHAISEN A, HOPPER N, KIM Y. Keep your friends close: Incorporating trust into social network-based sybil defenses[C]// 2011 Proceedings IEEE INFOCOM. IEEE, 2011: 1943-1951.

[11] NEWSOME J, SHI E, SONG D, et al. The sybil attack in sensor networks: analysis & defenses[C]//Third international symposium on information processing in sensor networks, 2004. IPSN 2004. IEEE, 2004: 259-268.

[12] LI F, MITTAL P, CAESAR M, et al. SybilControl: Practical Sybil defense with computational puzzles[C]//Proceedings of the seventh ACM workshop on Scalable trusted computing. 2012: 67-78.

[13] ZHANG K, LIANG X, LU R, et al. Sybil attacks and their defenses in the internet of things[J]. IEEE Internet of Things Journal, 2014, 1(5): 372-383.

[14] ZHOU T, CHOUDHURY R R, NING P, et al. P2DAP—Sybil attacks detection in vehicular ad hoc networks[J]. IEEE journal on selected areas in communications, 2011, 29(3): 582-594.

[15] HWANG J Y, CHEN L, CHO H S, et al. Short dynamic group signature scheme supporting controllable linkability[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(6): 1109-1124.

[16] MALANDRINO F, CASETTI C, CHIASSERINI C F, et al. A-VIP: Anonymous verification and inference of positions in vehicular networks[C]//2013 Proceedings IEEE INFOCOM. IEEE, 2013: 105-109.

[17] BOUASSIDA M S, GUETTE G, SHAWKY M, et al. Sybil Nodes Detection Based on Received Signal Strength Variations within VANET[J]. Int. J. Netw. Secur., 2009, 9(1): 22-33.