车载自组网Sybil攻击检测方案研究综述

李春彦 王良民

(江苏大学计算机科学与通信工程学院 镇江 212013)

摘 要 在车载自组网中,Sybil攻击是指恶意车辆通过伪造、偷窃或合谋等非法方式获取虚假身份并利用多个身份进行非正常行为而威胁到其他驾乘者生命财产安全的一种攻击。介绍了车载自组网中Sybil攻击的起因与危害,对Sybil攻击的检测方案进行了论述。根据检测过程是否与位置相关,将Sybil攻击检测方案分为与位置无关的检测方案和与位置有关的检测方案两类,对其中的检测方案进行了分类和比较。最后指出了现有方案中存在的问题和未来可能的研究方向。

关键词 车载自组网,Sybil攻击检测方案,Sybil攻击,与位置无关的检测方案,与位置有关的检测方案

中图法分类号 TP393 **文献标识码** A

Research on Detection Schemes of Sybil Attack in VANETs

LI Chun-yan WANG Liang-min

(School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract In vehicular ad hoc networks (VANETs) Sybil attack is an attack in which a malicious vehicle obtains multiple false identities through the way of forgery, stolen or conspiracy. The attacker uses these false identities to do misbehaviors which can threaten the lives and properties of other drivers and passengers. The cause and hazards of Sybil attack in vehicular ad hoc networks were introduced firstly. Then a survey of existing Sybil attack detection schemes was made. According as whether the detection process is related to positionthe detection schemes are classified into two categories: Non-position-based detection schemes and Position-based detection schemes. Comparison of detection schemes in each category was introduced elaborately as well. Finally, the problems in existing detection methods and some possible directions for future research were proposed.

Keywords Vehicular ad hoc networks, Sybil attack detection schemes, Sybil attack, Non-position-based detection schemes, Position-based detection schemes

1 引言

作为移动自组网(Mobile ad hoc networks, MANETs)在交通环境中的应用,车载自组网(Vehicular ad hoc networks-VANETs,以下简称车载网)旨在通过建立一个车辆间可以直接通信的平台,促进交通管理,增强道路安全,提高人们的出行质量[1,2]。但是由于短暂的通信时间、动态变化的拓扑结构、广播发送的消息及多跳传输的路由等特点[3,4]使得它易受到Sybil攻击的威胁。Sybil攻击最初是由Douceur在P2P网络中提出的[5],是一种基于身份的攻击,是指恶意节点通过非法方式获取多个虚假身份参与网络通信,以达到自己非法目的的一种攻击。在车载网中,Sybil攻击既能破坏消息的真实性,侵犯用户的隐私,又能破坏网络的可用性[6],具有极强的危害性。例如,Sybil攻击者可以利用多个虚假身份进行发送虚假交通信息、篡改消息等破坏消息真实性的攻击;在Sybil攻击的基础上,攻击者能够发动破坏用户隐私的攻击,如窃听用户隐私、泄露用户的路径信息等;另外,攻击者还能够发动破坏网络可用性的重放攻击、黑洞攻击、虫洞攻击、DOS攻击和选择性转发攻击等。这些攻击行为直接或间接地威胁着其他驾乘者的生命财产安全,影响了网络的正常运作,给车载网的发展和普及带来了巨大的障碍。

关于车载网的安全技术,目前已有较为全面的研究[7-9],但是针对其中的Sybil攻击问题,还没有相关的综述。为此本文综述了车载网中的Sybil攻击检测方案,根据不同方案检测过程中是否与位置相关,分为与位置无关的检测方案和与位置有关的检测方案。本文第2节概述了车载网的网络结构和Sybil攻击在车载网中的主要危害;第3节详述了与位置无关的检测方案;第4节介绍了与位置相关的检测方案;第5节对上述检测方案进行了分析和对比;最后对文章进行了总结,指出了现有方案中存在的问题,并提出了未来可能的研究方向。

2 背景知识

简单介绍了典型的车载网网络模型,概述了Sybil攻击

本文受国家自然科学基金(61272074),江苏省自然科学基金(BK2011464),镇江市工业科技支撑项目(GY2013030)资助。

李春彦(1988—),女,硕士生,主要研究方向为车载自组网入侵检测技术,E-mail:lcy20110416@163.com;王良民(1977—),男,博士,教授,博士生导师,主要研究方向为物联网安全与应用。

在车载网中的危害。文中将发动 Sybil 攻击的车辆称为恶意车辆、恶意节点或 Sybil 攻击者，使用虚假身份的车辆称为 Sybil 车辆或 Sybil 节点。

2.1 网络模型

文章采用典型的层次式车载网结构，如图 1 所示。每个车辆都有车载单元(on Board Unit，OBU)，用来实时采集自身的交通信息，如位置、速度和方向等。路旁单元(Road Side Unit，RSU)是无线通信的物理基站，为车辆接入其他固定的或移动通信网络提供相关服务上的支持。可信结构(Trusted Authority，TA)一般由政府部门承担，存储网络中所有车辆的信息，并认为它有足够的存储空间，且不可被敌人摧毁。网络中的通信方式主要包括车与车之间的通信(Vehicle to Vehicle，V2V)和车辆与基础设施之间的通信(Vehicle to Infrastructure，V2I)。V2V 通信允许车辆之间不借助基础设施直接相互收发信息，提前告知其他车辆本地的交通信息。V2I 通信通过 RFID[10] 等技术为车辆接入其他固定的网络提供方便，也可用于车辆身份的分发、管理和撤销等应用。

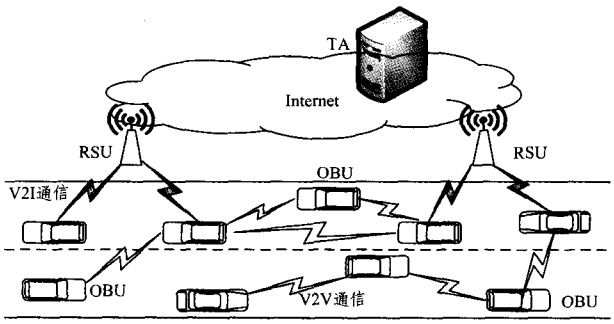

图 1 VANETs 结构

2.2 Sybil 攻击的危害

车载网不仅具有传统分布式网络无中心、自组织的特点，还有许多独有的特点，例如车辆的运动情况受道路状况、天气环境和交通规则的限制等，这些特点使得它更易受到 Sybil 攻击的威胁，Sybil 攻击者可以使用多个虚假身份进行以下多种攻击。

2.2.1 伪造交通场景

恶意车辆可以利用多个身份发送虚假消息，伪造交通场景[11]，如图 2 所示。为独享道路，车辆 A 通过伪造 Sybil 节点，发送多个虚假位置消息，使得正常车辆 B 认为前方发生交通拥堵，从而绕路行驶。同样，恶意车辆可以使用类似的方法，制造 Sybil 车辆顺利通过交通拥堵区域的假象，混淆后续车辆的判断能力，导致司机做出错误的决定，使交通更加拥堵甚至引发车辆连环相撞，直接威胁到其他驾乘者的生命财产安全。

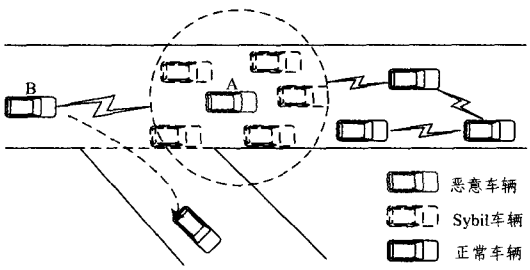

图 2 Sybil 攻击伪造交通拥堵

2.2.2 破坏投票机制

为增强网络的安全性，一些研究者提出建立信誉系统的方法[12,13]为每个节点建立信任值表示它的可信度，使用投票机制更新信任值的大小。然而，恶意节点可以利用 Sybil 攻击堵塞投票箱破坏投票机制，或者利用所拥有的多个 Sybil 节点发送虚假投票信息改变投票结果。

2.2.3 破坏路由协议

恶意车辆可以破坏车载网中的某些路由协议[14,15]，例如在基于地理位置的路由[16]中，一个恶意节点可能同时以不同的身份出现在多个地理位置，使得基于地理位置的路由经过不同地理位置的多个 Sybil 节点建立路由。如图 3 所示，恶意节点 A 伪造身份 A1、A2、A3，并将自己的位置和 3 个虚假位置广播给周围的节点，正常节点 B 收到广播信息后，存储每个节点及其位置。当 B 发送消息给节点 C 时，会选择距离节点 C 最近的节点 A2 作为中间节点，这样恶意节点 A 就成功截获了节点 B 发送给节点 C 的所有消息，破坏了网络原有的路由协议。

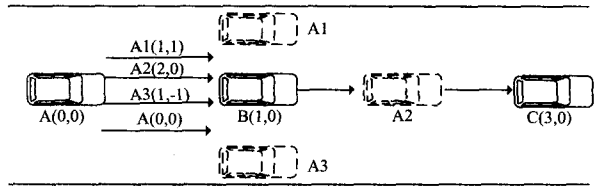

图 3 Sybil 攻击破坏路由协议

另外，恶意车辆还可以通过非法收集消息，获取驾驶者的行程信息或盗取其加油卡密码等，侵犯用户的隐私。同时，Sybil 攻击者可以使用拥有的多个虚假身份同时发送消息使信道发生拥堵，引发 DOS 攻击，或通过使用虚假身份向网络中注入虚假消息、篡改消息、重放消息等方式进行攻击。

3 与位置无关的检测方案

与位置无关的 Sybil 攻击检测方案包括基于资源的检测方案、基于密码认证的检测方案、针对滥用假名的 Sybil 攻击检测方案和其他检测方案 4 种，如图 4 所示。本节详细介绍了这些检测方案，并指出了各类方案的优缺点。

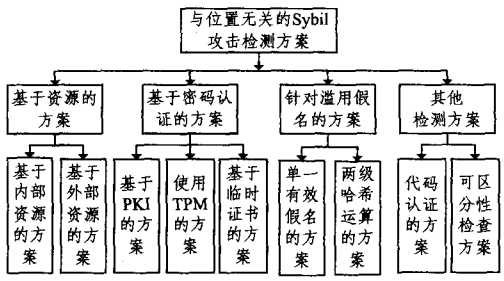

图 4 与位置无关的 Sybil 攻击检测方案分类

3.1 基于资源的检测方案

恶意车辆利用虚假身份发动 Sybil 攻击，需要利用并消耗自身的一些资源，因此许多研究者提出从节点拥有资源的角度抑制 Sybil 攻击。节点的资源既包括节点的计算能力、通信能力、存储能力和通信模块等内部资源，也包括节点的社会关系和节点进行通信所需要付出的费用等外部资源。

3.1.1 基于内部资源的检测方案

Douceur 最先在文献[5]中提出了资源测试的方法，该方法中假设每个节点拥有的内部资源是有限且完全相同的，验证者通过验证某个身份对应的实体是否具有独立实体应当具

备的能力找到 Sybil 节点。例如当节点的计算资源有限时，为验证某个节点是否为 Sybil 节点，验证节点向该节点发送计算难题，如果该节点是 Sybil 节点，那么它将不能按时给出难题正确的解决方案。但是当存在多个被验证节点时，上述操作必须同时进行，否则恶意节点可以分时利用自己的资源，导致检测方案失效。但是这种要求是很难实现的。Newsome 等在文献[17]中指出资源测试的方法不能用于无线传感器网络，因为在无线传感网中恶意节点可以轻易获取更多的资源，并且文献[5]中测试节点通信能力的方法会引起网络拥堵。他们提出了无线资源测试的方法，即假设每个节点仅有一个无线通信模块，该模块不能在多个信道上同时收发消息，从而限制了一个节点一次只能以一个身份发送消息。但是该方法不能用于自组网，因为在自组网中，恶意车辆可以轻易获取多个无线通信模块。

3.1.2 基于外部资源的检测方案

Yu H 和 Danezis G 等人提出使用社交网络抵御 Sybil 攻击的方法[18,19]。该方法利用节点之间的“社会关系”限制 Sybil 攻击的规模，它的基本思想是恶意节点可以伪造多个虚假身份，但是不能伪造虚假身份与正常节点之间的关系，然而正常节点之间可以通过相互通信快速建立关系。该方法通过节点之间的强信任关系，限制了受 Sybil 节点影响的正常节点的数量，抑制了 Sybil 攻击的规模。但是该方法不适用于车载网中，因为车辆不断运动，使得网络拓扑结构频繁变化，节点之间不易建立长期稳定的关系。

Margolin 等在文献[20]中对 Sybil 攻击进行了经济分析，假设每个恶意节点都是理性的，那么它的攻击收益要大于攻击成本。通过对每个参与身份进行重复收费的方法，从经济学的角度抑制 Sybil 攻击。这种方法能够限制 Sybil 攻击的规模，但是也抑制了正常节点参与通信的积极性，不适用于消息广播发送的车载网。

3.2 基于密码认证的检测方案

基于密码认证的检测方案通常需要一个权威中心为每个入网车辆分发唯一密钥或证书，依赖于车辆和密钥或证书之间的一一对应关系来抵御 Sybil 攻击。这种方法的优点是能够较强地抵御 Sybil 攻击，缺点是网络扩展性差，存在隐私泄露问题和恶意节点的证书撤销问题，网络开销大。

3.2.1 基于 PKI 的检测方案

为了防止恶意车辆对自己发送的虚假消息进行抵赖，文献[21-23]中提出使用密钥加密的方法。车辆使用私钥签署消息并附加相关证书，接受者使用相应的公钥解密，由于身份和密钥的对应关系，该方法能够抵御伪造身份的 Sybil 攻击。另外，为保护车辆的隐私，文献[21]中提出了条件性匿名的方法，并解决了密钥的分发、存储和撤销等问题。但是，基于 PKI(Public Key Infrastructure)的方法具有较高的计算开销，且密钥的更换需要基站的在线支持。文献[23]中使用固定的密钥设施为每个车辆生成公/私钥对，通过解密和哈希的方式验证消息的有效性和完整性。该方法可以抵御 Sybil 攻击，但是存在性能瓶颈，且容易泄露用户的隐私。基于 PKI 的检测方案的优点是有能力消除 Sybil 攻击，缺点是需要中心基站的支持，并且存在密钥的管理问题和撤销问题，还可能会泄露用户的隐私信息。

3.2.2 使用 TPM 的检测方案

Guette 等提出了一种基于可信平台模块(Trust Platform Module，TPM)保护车载网的方法[24]。该方法中每辆车都内嵌一个 TPM，它有唯一的认证密钥存储在持久性存储器(Non-volatile Storage)中，且密钥的公共部分为其他 TPM 所知。车辆之间首先通过汽车权威部门为 TPM 生成的平台信任凭证建立可信信道，然后通过挑战-应答协议验证信息。该方法中的 TPM 实质是证书的变体，它的优点是可靠性高，缺点是需要较多的人工参与和特殊硬件支持，检测成本高。

3.2.3 使用临时证书的检测方案

如果能够保证在某个特定的时间和地点每个车辆只有一个有效的密钥对和证书，那么就能够有效抵御 Sybil 攻击。基于这种思想，Park 等在文献[25]中提出了一种基于临时证书(Temporary Certificate-based Approach，TCA)抵御 Sybil 攻击的方法。为保证每个车辆只有一个证书，在初次发放证书时，需要带有“相机”的 RSU 对车辆进行物理验证。之后车辆在遇到新的 RSU 时需要请求更新临时证书，获得新的临时证书后，原有的证书就会失效。这种方法的优点是能够抵御伪造临时证书的 Sybil 攻击，缺点是当车辆初次进入网络时，只有遇到具有“相机”的 RSU，才能获得临时证书和密钥。另外，当 RSU 被 Sybil 攻击者俘获时，该方法将彻底失效。

3.3 针对滥用假名的 Sybil 攻击检测方案

由于上述一些检测方案存在泄露用户隐私的风险，许多研究者提出使用假名机制解决网络的隐私保护问题[26-31]。但是某些恶意车辆对假名的非正常使用(使用多个假名发送相同或类似的消息)带来了 Sybil 攻击的隐患。

3.3.1 基于单一有效假名的检测方案

针对恶意车辆滥用假名引起的 Sybil 攻击问题，文献[26]中提出了一种轻量级的解决方案。车辆一次只能拥有一个有效假名，在这个假名即将失效前，车辆通过请求 TA 或 RSU 在线获得新的有效假名，因此抵御了滥用假名引起的 Sybil 攻击，也保护了用户的隐私。但是车辆更新假名时需要基站的在线支持，如果没有基站的帮助，车辆将无法获得新的假名，无法发送信息。另外，恶意节点可以利用俘获的 RSU 给其他恶意车辆发送多个有效假名，而给正常车辆发送无效假名或不给正常车辆发送假名。

3.3.2 利用两级哈希运算的检测方案

为解决滥用假名带来的 Sybil 攻击，Zhou Tong 等提出了一种新的假名分配机制 P^2DAP[31]。该方法中 TA 通过使用粗粒度密钥 K_c 和细粒度密钥 K_f 分别对假名进行哈希计算得到假名的粗粒度哈希值和细粒度哈希值。一个粗粒度群内所有车辆的粗粒度哈希值相同，细粒度哈希值不同，但是一个车辆所有假名的细粒度哈希值相同。为应对被俘获的 RSU，TA 仅将粗粒度密钥 K_c 发送给 RSU。收到周围车辆发送的消息后，RSU 计算假名的粗粒度哈希值，如果两个假名的粗粒度哈希值相同，则对应的两条消息可能由同一辆车发送，也可能是由同一粗粒度群内的不同车辆发送的。RSU 将假名和计算得到的粗粒度哈希值发送给 TA，TA 通过计算它们的细粒度哈希值，可以判定是否存在 Sybil 车辆。这种方法的优点是能够保护车辆的隐私，应对被俘获的 RSU，检测到恶意车辆滥用假名的 Sybil 攻击行为，缺点是当车辆之间传送的消息较多时，RSU 和 TA 需要多次计算假名的粗粒度哈希值和细粒度哈希值，给网络带来了较大的计算开销。

3.4 其他检测方案

3.4.1 代码认证的检测方案

Newsome 等在文献[17]中提出了代码认证的 Sybil 攻击检测方案，该方案的基本思想是恶意节点和正常节点内部运行的代码不同，因此可以通过验证节点的内存代码判断节点是否是恶意节点。这种方法的优点是能够抵御多种类型的攻击，缺点是费用高，能量损耗大，在大规模的车载网中使用不现实，可行性差。

3.4.2 可区分性检查的检测方案

通过建立网络的正常模型[32]，或依据攻击特征建立攻击模型[33]，将网络实际情况与所建模型进行对比来检测恶意行为，保护车载网安全的方法，称为可区分性检查(Distinguishability Detection，DD)的方法。

通过集成不同传感器的消息构建网络安全模型，并使用该模型识别恶意消息和恶意节点[32]。当网络中存在 Sybil 攻击时，网络模型会发生异常，通过与安全模型进行比较就可以检测到网络中的异常节点，但是为大规模的车载网建立一个完整的安全模型是非常困难的。文献[33]中利用机器学习的方法建立一个区分恶意节点和正常节点的安全框架，根据发动攻击时车辆的具体行为特征(车辆的速度偏差、RSSI、传送包的数量等)对车载网中的恶意行为进行分类。依据发动 Sybil 攻击时车辆的行为特征，将攻击模型、车载网模型和收到的包的特征使用分类算法进行分类，可以判断网络中是否存在这种攻击。该方法的优点是检测结果不受 Sybil 攻击中虚假身份来源的影响，缺点是只能检测网络中已知的攻击行为，且检测效果取决于分类算法的性能。

4 与位置有关的检测方案

与位置有关的检测方案包括基于邻居车辆的检测方案、基于车辆路径信息的检测方案、基于收到的信号强度(Received Signal Strength Indication，RSSI)的检测方案和基于位置合理性的检测方案，如图 5 所示。它们都与车辆的位置有关，但是依据的思想不同。第一种方案依据的思想是不考虑堵车的情况下，车辆在相当长时间内不会一直拥有相同的邻居节点；第二种检测方案的思想是所有车辆在独立运动的情况下，它们的运动路径在一段时间内不会是完全相同的；第三种检测方案的思想是攻击者虽然可以借助 Sybil 身份发送多个虚假消息，但是这些消息来源的位置都是相同的；第四种检测方案通过车辆之间合作分析可疑车辆的位置是否合理来找到 Sybil 节点。

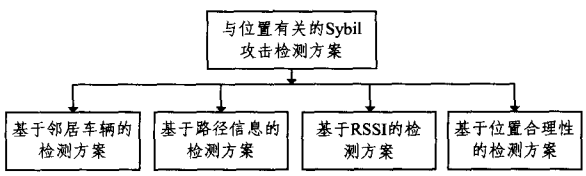

图 5 与位置有关的 Sybil 攻击检测方案分类

4.1 基于邻居车辆的检测方案

由于车辆的不断运动(不考虑堵车和车队情况)，在一段时间内，车辆之间不会一直拥有许多相同的邻居车辆(Neighboring Vehicle，NV)。基于这种思想，Grover[34] 等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。该方法中每个节点周期性广播指示消息告知周围车辆自己的信息，同时接收指示信息，得到自己的邻居节点集合。之后和周围的车辆交换邻居节点集合，并计算集合的交集。如果在一段时间 σ 内，所有车辆的邻居节点中始终有相同的车辆，那么这些相同的车辆就被认为是 Sybil 车辆。

这种检测方案的优点是不需要 RSU 的帮助，也不需要交换车辆的私密信息(位置、速度等)，但是要合理设置时间 σ 的大小。σ 如果太大，就会检测不到攻击时间小于 σ 的 Sybil 攻击；如果太小，又会引起较高的误报率。另外该方法需要假设多数邻居车辆是正常车辆，这本身就是一个检测悖论。

4.2 基于路径信息的检测方案

考虑到车辆运动的自主性，网络中没有任何两个车辆会在一段时间内的相同时刻经过相同的 RSU，且一个车辆也不可能同时出现在不同的 RSU 处。但是恶意车辆和 Sybil 车辆却始终具有完全相同的运动路径。基于这种思想，许多研究者提出了基于车辆路径信息的 Sybil 攻击检测方案。

在城市车载网中，道路交叉处有固定的 RSU 为车辆提供额外的服务，假设它们完全可信，并周期性地广播含有时间戳的签名向量。车辆从 RSU 通信范围内经过时接收并保存这些签名向量，然后观察车辆通过收集并计算所有邻居节点签名向量的不同，判断邻居节点中是否存在 Sybil 节点[35]。如图 6 所示，假设车辆 A、B 为正常车辆，车辆 C 和 C′分别是恶意车辆和 Sybil 车辆。通过表 1 可以看到，车辆 C 和 C′的运动路径在 t_1-t_5 时间内完全相同，因此可以认为它们中存在 Sybil 车辆。这种方法的优点是简单易行，具有较高的检测率和健壮性；缺点是没有考虑到恶意车辆修改签名向量的情况，同时恶意车辆通过路径信息可以追踪其他车辆，泄露车主的行程信息。与上述方法相比，文献[25]中的方法增强了车辆和 RSU 的通信安全性，防止了恶意车辆滥用窃听的签名向量再次发动 Sybil 攻击的行为。车辆在请求新的 RSU 签名和进行 V2V 通信时，需要发送先前一段时间内收到的签名，以证明自己具有合法身份。这虽然增强了通信的安全度，但是也导致了车辆的位置隐私和路径信息的泄露，并且文中没有考虑在 RSU 覆盖重叠区域签名向量的发送情况。

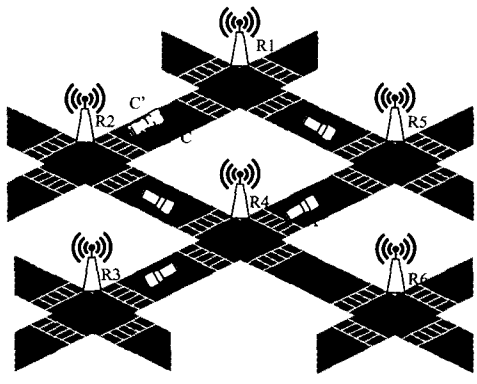

图 6 某一个时刻交通图

表 1 车辆 O 的邻居节点路径信息收集表

时间	节点 A	节点 B	节点 C	节点 C′
t_1	R5	R6	R4	R4
t_2	R6	R3	R5	R5
t_3	R6	R3	R5	R5
t_4	R3	R2	R1	R1
t_5	无	R4	R2	R2

Footprint[36]沿用并扩展了文献[25,35]中的方法，车辆主动请求 RSU 发送带有时间戳的数字签名，并将这些签名作为自己的身份，通过对比所有邻居车辆身份的一致性检测 Sybil 节点，解决了车辆篡改中间签名的问题。RSU 发送路径信息时采用环签名机制实现了模糊签名和签名的短时链接性，保护了车辆的位置隐私和路径信息，实现了 Sybil 攻击的在线检测。该方法同样要求 RSU 是完全可信的，无法抵御 RSU 被俘获的攻击，也无法抵御合谋 Sybil 攻击（两个或多个恶意车辆合谋将自己的路径信息提供给某个恶意车辆，该车辆向 RSU 发送多个路径信息请求签名的攻击）。

4.3 基于 RSSI 的检测方案

一个身份只能有一个位置，同样一个相对精确的位置只能有一辆车。文献[37]中通过实验证明恶意节点增强传输功率并没有增大攻击成功域，反而有利于正常节点的检测，因此可以利用 RSSI 估计消息的发送位置。

Yu Bo 等利用预设的无线信号传播模型和 RSSI 分布模型计算邻居节点的估计位置[38]，如果估计位置与其发送的数据包中的位置不同，那么该节点可能是发送虚假位置伪造交通场景的 Sybil 节点。该方法在 RSU 的帮助下选用反向车辆作为证明车辆，消除了证明车辆中的 Sybil 车辆。然而，这也导致该方法不能用于单向道路环境中，且对车辆的密度要求较高，另外预定的信号传播模型和信号分布模型在某些车载网环境中可能并不适用。

文献[39]提出的方法中节点将自己的位置发给邻居节点，邻居节点利用 RSSI[38,40,41]或者根据文献[42]中基于多个传感器验证位置的方法估计发包车辆的位置，如果估计位置与包中位置有显著差异，说明发包车辆发送了虚假的位置信息，则拒绝接收该车辆的消息，否则在观察表中存储相应的位置和时间。如果观察表中存在两行或多行内容相同，那么这些行对应的节点就是 Sybil 节点。这种方法利用其它文献中的方法验证车辆的位置，但是文中没有提到怎样验证车辆的身份，也没有提出具体的解决方案。

4.4 基于位置合理性的检测方案

在隐私保护的车载网中，Hao Yong 等在文献[43]中提出了一种合作型 Sybil 攻击检测方案（Cooperative Sybil Attack Detection，CSAD）。该方案中，车辆在局部范围内通过合作验证车辆位置的合理性找到 Sybil 节点。该方法的优点是不需要特殊硬件和 RSU 的支持，具有较低的通信开销和计算开销，但是当恶意车辆和 Sybil 车辆在局部区域中占有比例较大时，该方法将会失效。另外，该方法本身没有考虑车辆的隐私问题，容易泄露车辆的位置隐私和路径信息。

5 综合比较

在第 3 节和第 4 节中分别介绍了与位置无关的和与位置有关的 Sybil 攻击检测方案，表 2 从能够检测到的 Sybil 攻击类型[17]、安全性和检测过程是否需要 RSU 的辅助作用 3 个方面对上述检测方案进行了对比（由于基于资源的检测方案和代码认证的检测方案不适用于车载网，因此没有列入对比）。其中安全性包括完整性（消息的完整性）和隐私性（做到了隐私保护），√表示能够检测到对应的攻击类型或满足对应要求，×表示不能检测到对应的攻击类型或不满足对应要求，Δ表示没有考虑对应的要求。NV[34]检测方案中假设大多数邻居节点都是正常节点。

表 2 车载网中 Sybil 攻击检测方案的对比

检测方案		能够检测到的 Sybil 攻击类型						安全性		需要 RSU
		直接通信	间接通信	伪造身份	偷窃身份	同时参与	非同时参与	完整性	隐私性	
与位置无关的检测方案	PKI[19]	√	×	√	×	√	√	√	×	√
	TPM[20]	√	×	√	×	√	√	√	×	×
	TCA[25]	√	×	√	×	√	√	√	×	√
	P²DAP[31]	√	×	√	×	√	×	Δ	√	√
	DD[33]	√	√	√	√	√	√	Δ	Δ	√
与位置有关的检测方案	NV[34]	√	√	√	√	√	×	Δ	×	×
	FOOT[36]	√	×	√	×	√	×	√	√	√
	RSSI[38]	√	×	√	√	√	√	Δ	×	√
	CSAD[43]	√	×	√	√	√	×	Δ	×	×

从表 2 可以看出，现有的检测方案多数利用了车载网特有的网络结构，在检测过程中需要 RSU 的辅助作用，并且这些方案在理想情况下基本都可以检测到直接通信、伪造身份和同时参与的 Sybil 攻击，但是多数不能检测到间接通信的 Sybil 攻击和偷窃身份的 Sybil 攻击。其中基于 RSSI 的 Sybil 攻击检测方案能够检测到多种类型的 Sybil 攻击，是一种很有前景的方法，提高其定位的精确度将是未来研究的一个重要方向。基于车辆路径信息的检测方案能够满足多种要求，检测思想简单易行，并且假设 RSU 的可信性在多数情况下是合理的。可区分性检查方案虽然检测效果好，但是成本较高，并不适合用于大规模的车载网中。

结束语 本文针对车载网中的 Sybil 攻击问题，论述了它能够带来的危害，对其检测方案的研究现状进行了详细的介绍和分析。从综合比较中可以发现，现有的 Sybil 攻击检测方案存在以下问题：

1）与位置有关的检测方案多数存在泄露车辆位置隐私的风险，而与位置无关的检测方案易受 Sybil 攻击中虚假身份的来源形式的影响。多数检测方案无法抵御间接通信的 Sybil 攻击、偷窃身份的 Sybil 攻击和非同时参与攻击。

2）某些检测方案没有充分考虑到车载网的特点，可能并不适用于车辆运动速度较快的大规模车载网环境。

3）一些检测方案存在潜在 Sybil 攻击的可能，Sybil 攻击者会利用检测方案的特点，发送虚假信息，影响检测方案的性能。另外某些检测方案虽然检测效果好，但是需要特殊硬件

的支持，系统开销大，投入成本高。

因此，在未来的 Sybil 攻击检测方案中，我们认为将会有以下发展趋势：

1)根据特殊情况需求，制定与位置有关的检测方案或与位置无关的检测方案。研究与虚假身份来源无关、通信方式无关的 Sybil 攻击检测方案，提高利用 RSSI 或传感器定位恶意节点的精确度将是未来研究的一个重要方向。

2)在智能交通系统的蓬勃发展下，基站的全面覆盖和完全可信将成为现实，充分利用 RSU 的辅助作用是未来 Sybil 攻击检测方案的重要手段。

3)研究节点独立执行的检测方案，去除潜在 Sybil 攻击的可能。生产高性能设备，降低检测成本，做好系统安全和隐私保护的平衡、系统开销和检测效率的平衡是未来 Sybil 攻击检测方案的目标。

参 考 文 献

[1] Blum J, Eskandarian A, Hoffman L. Challenges of inter-vehicle ad hoc networks [J]. IEEE Transactions on Intelligent Transportation Systems, 2004, 5(4): 347-351

[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): 116-127

[3] 乔震，刘光杰，李季，等. 移动自组织网络安全接入技术研究综述[J]. 计算机科学，2013, 40(20): 1-9

[4] 王良民，李晓君，仲红. VANET 中一种可撤销的车辆群组批认证方法 [J]. 中国科学：信息科学，2013, 43(10): 1307-1325

[5] Douceur J R. The Sybil attack [C]// Proceeding of International Workshop on Peer-to-peer Systems. Cambridge. USA, IEEE, 2002: 251-260

[6] Razzaque M A, Salehi A, Cheraghi S M. Security and privacy in vehicular Ad-Hoc networks: survey and the road ahead [M]// Wireless Networks and Security. Springer Berlin Heidelberg, 2013: 107-132

[7] Hartenstein H, Laberteaux K P. A tutorial survey on vehicular ad hoc networks [J]. Communications Magazine, IEEE, 2008, 46(6): 164-171

[8] Lacroix J, El-Khatib K. Vehicular Ad Hoc Network Security and Privacy: A Second Look [C]// The Third International Conference on Advances in Vehicular SystemsTechnologies and Applications(VEHICULAR 2014). 2014: 6-15

[9] Al Sultan S, Al Doori M M, Bayatti A H, et al. A comprehensive survey on vehicular Ad Hoc network [J]. Journal of Network and Computer Applications, 2014, 37: 380-392

[10] 王良民，茅冬梅，梁军. 基于 RFID 系统的隐私保护技术[J]. 江苏大学学报：自然科学版，2012, 33(6): 690-695

[11] Bissmeyer N, Stresing C, Bayarou K M. Intrusion detection in VANETs through verification of vehicle movement data [C]// Vehicular Networking Conference (VNC) 2010. New Jersey, USA, IEEE, 2010: 166-173

[12] Ding Qing, Li Xi, Jiang Ming, et al. Reputation-based trust model in vehicular ad hoc networks [C]// International Conference on Wireless Communications and Signal Processing (WCSP). Suzhou, China, 2010: 1-6

[13] Chen Yi-ming, Wei Yu-chih. A beacon-based trust management system for enhancing user centric location privacy in VANETs [J]. Journal of Communications and Networks, 2013, 15(2): 153-163

[14] Korkmaz G, Ekici E, Ozguner F, et al. Urban multi-hop broadcast protocol for inter-vehicle communication systems [C]// Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks. Philadelphia, PA, USA, ACM, 2004: 76-85

[15] Zhao Jing, Cao Guo-hong. VADD: Vehicle-assisted data delivery in vehicular ad hoc networks [J]. IEEE Transactions on Vehicular Technology, 2008, 57(3): 1910-1922

[16] Karp B, Kung H T. GPSR: Greedy perimeter stateless routing for wireless networks [C]// Proceedings of the 6th Annual International Conference on Mobile Computing and Networking. Boston, MA, USA, ACM, 2000: 243-254

[17] Newsome J, Shi E, Song D, et al. The Sybil attack in sensor networks: analysis & defenses [C]// Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks. Berkeley, California, USA: ACM, 2004: 259-268

[18] 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

[19] Danezis G, Mittal P. SybilInfer: Detecting Sybil Nodes using Social Networks [C]// Proceedings of the Network and Distributed System Security Symposium. San Diego, California, USA, 2009: 1-15

[20] Margolin N B, Levine B N. Quantifying resistance to the Sybil attack [M]// Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2008: 1-15

[21] Raya M, Hubaux J P. Securing vehicular ad hoc networks [J]. Journal of Computer Security, 2007, 15(1): 39-68

[22] 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：工学版，2013, 43(6): 14-19

[23] Rahbari M, Jamali J. Efficient detection of Sybil attack based on cryptography in VANET [J]. International Journal of Network Security & its Applications (IJNSA). 2011, 3(6): 185-195

[24] Guette G, Bryce C. Using TPMs to secure vehicular ad-hoc networks (VANETs) [M] // Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks. Springer Berlin Heidelberg. 2008: 106-116

[25] Park S, Aslam B, Turgut D, 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

[26] Studer A, Shi E, Bai F, et al. TACKing together efficient authentication, revocation, and privacy in VANETs [C]// 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks(SECON09). Rome, Italy, IEEE, 2009: 1-9

[27] Sun Yi-pin, Lu Rong-xing, Lin Xiao-dong, et al. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications [J]. IEEE Transactions on Vehicular Technology, 2010, 59(7): 3589-3603

(下转第 262 页)

结果误差依然保持快速上升的趋势且偏离实际较多。方案2采用灰色Verhulst传统模型，预测结果同样偏离实际值较多，误差依然很大，新建的模型最贴近实际值，误差小，精度高。

结束语 自适应灰色参数克服了使用传统模型在决定参数系数和提高精度上的不足。通过使用新的预测结果替换原始序列中的第一个元素，这有益于所提出的预测模型及时辨别曲线变化趋势，而使传统序列的维度更加稳定，这个方法使得新建模型能更准确预测曲线的趋势和提高预测精度。

本文虽已分析和讨论了单峰态势的变化情况，并且改进了灰色Verhulst模型，但需要注意的是更为常见的多峰态势变化。在未来的研究中，将更加注重研究分析多峰态势变化以及预测复杂态势变化。

参 考 文 献

[1] 王慧强. 网络安全态势感知研究新进展[J]. 大庆师范学院学报，2010，30(3)：1-8

[2] 李颖. NSSA中网络安全态势预测研究[J]. 技术与市场，2010，17(12)：43-44

[3] 赵嶷飞，史永亮. 基于模糊综合评价的航路交通态势评估[J]. 中国民航大学学报，2011，29(1)：5-8

[4] Bass T. Intrusion detection systems and multi. Sensor data fusion：Creating cyberspace situational awareness [J]. Communications of the ACM，2000，43(4)：99-105

[5] Ren W，Jiang X H，Sun T F. Rbfnn. based prediction of networks security situation [J]. Computer engineering and Applications，2006，42(31)：136-139

[6] Lai J B，Wang H Q，Zhao L. Study of network security situation awareness model based on simple additive weight and grey theory[C]//Proceedings of 2006 International Conference on Computational Intelligence and Security. Hangzhou：IEEE Press，2006：1545-1548

[7] 邓聚龙. 灰色预测与决策[M]. 武汉：华中科技大学出版社，2002

[8] 邓聚龙. 灰色系统基本方法[M]. 武汉：华中科技大学出版社，1987

[9] Liu S F，LIN Y. An introduction to grey systems theory [M]. Grove City：IIGSS Academic Publisher，1998

[10] Guo Z J，Song X Q，YE J. A Verhulst model on time series error corrected for port throughput forecasting[J]. Journal of the Eastern Asia Society or Transportation Studies，2005(6)：881-891

[11] 傅立. 灰色系统理论及其应用[M]. 北京：科学文献出版社，1992

(上接第240页)

[28] Ruj S，Cavenaghi M A，Huang Z，et al. On data-centric misbehavior detection in VANETs [C]//Vehicular Technology Conference (VTC Fall). San Francisco，CA，USA，IEEE，2011：1-5

[29] Lu Rong-xing，Li Xiao-dong，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

[30] Pan Yuan-yuan，Li Jian-qing，Feng Li，et al. An analytical model for random pseudonym change scheme in VANETs [J]. Cluster Computing，2013：1-9

[31] Zhou Tong，Choudhury R R，Ning Peng，et al. P2DAP—Sybil Attacks Detection in Vehicular Ad Hoc Networks [J]. IEEE Journal on Selected Areas in Communications，2011，29(3)：582-594

[32] Golle P，Greene D，Staddon J. Detecting and correcting malicious data in VANETs [C]//Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks. Philadelphia，PA，USA，ACM，2004：29-37

[33] Grover J，Prajapati N K，Laxmi V，et al. Machine learning approach for multiple misbehavior detection in VANET [M]// Advances in Computing and Communications. Springer Berlin Heidelberg，2011：644-653

[34] Grover J，Gaur M S，Laxmi V，et al. A Sybil attack detection approach using neighboring vehicles in VANET [C]//Proceedings of the 4th International Conference on Security of Information and Networks. Sydney，Australia，ACM，2011：151-158

[35] Chen Chen，Wang X，Han Wei-li，et al. A robust detection of the Sybil attack in urban VANETs [C]//The 29th IEEE International Conference on Distributed Computing Systems Workshops(ICDCS 2009). Montreal，Quebec，Canada，IEEE，2009：270-276

[36] Chang Shan，Qi Yong，Zhu Hong-zi，et al. Footprint：detecting Sybil attacks in urban vehicular networks [J]. IEEE Transactions on Parallel and Distributed Systems，2012，23(6)：1103-1114

[37] Guette G，Ducourthial B. On the Sybil attack detection in VANET [C]// IEEE International Conference on Mobile Ad hoc and Sensor Systems(MASS 2007). Pisa，Italy，IEEE，2007：1-6

[38] Yu Bo，Xu Cheng-zhong，Xiao Bin. Detecting Sybil attacks in VANETs [J]. Journal of Parallel and Distributed Computing，2013：746-756

[39] Grover J，Kumar D，Sargurunathan M，et al. Performance evaluation and detection of Sybil attacks in vehicular ad-hoc networks [M]// Recent Trends in Network Security and Applications. Springer Berlin Heidelberg，2010：473-482

[40] Capun S，Hubaux J P. Secure positioning of wireless devices with application to sensor networks [C]// Proceeding of 24th Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM 2005). Miami，USA，IEEE，2005：1917-1928

[41] Bouassida M S，Guette G，Shawky M，et al. Sybil nodes detection based on received signal strength variations within VANET [J]. IJ Network Security，2009，9(1)：22-33

[42] Leinmuller T，Schoch E，Kargl F. Position verification approaches for vehicular ad hoc networks [J]. IEEE Wireless Communications，2006，13(5)：16-21

[43] Hao Yong，Tang Jin，Cheng Yu. Cooperative Sybil attack detection for position based applications in privacy preserved VANETs[C]// Global Telecommunications Conference (GLOBECOM 2011). Houston，Texas，USA，IEEE，2011：1-5