VANETs 中基于时空分析的抗合谋 Sybil 攻击检测方法

石亚丽 王良民

(江苏大学计算机科学与通信工程学院 江苏 镇江 212013)

摘 要 在车载自组网中,攻击者通过伪造、偷窃以及与其它合法车辆合谋等方式获得多个网络身份,并利用这些身份发布虚假交通信息来伪造交通场景,从而造成交通拥堵,甚至引发更严重的交通事故.现有的多数 Sybil 攻击检测方案主要用于检测伪造身份或偷窃身份的 Sybil 攻击,很少有检测方案针对合谋 Sybil 攻击进行研究.另外,检测 Sybil 攻击需要确保车辆实体在网络通信时仅绑定一个网络身份以防止攻击者扮演多个身份来欺骗其他车辆,这种做法会造成车辆隐私的泄露.为了平衡解决 Sybil 攻击检测和隐私保护这两个相互矛盾的问题,该文提出了一种基于时空分析的抗合谋 Sybil 攻击检测方法 STARCS(Spatio-Temporal Analysis based Resist Conspiracy Sybil Attack).该方法利用匿名 RSU 发布的时间戳标识作为车辆在车载自组网中的身份,通过权威机构 TA(Trust Authority)设置的请求信息表记录前一次经过的 RSU 和时间戳,从而抵御伪造 Sybil 身份和合谋 Sybil 身份的产生.文中每个警报事件只允许每个车辆发布一次带有时间戳标识的警报消息,根据警报信息中包含的标识是否被多个车辆同时使用来检测攻击者与合谋车辆同时使用同一身份的合谋 Sybil 攻击,并依据标识中嵌入的 RSU 位置关系标签检测攻击者与远距离车辆合谋的 Sybil 攻击.由于从时间上身份是否被滥用和空间上身份是否出现不合理位移的情况来检测合谋 Sybil 攻击,即是从时空关系上抵制和检测合谋 Sybil 攻击.理论分析和仿真实验表明,该方法不仅能够抵御或检测多种 Sybil 攻击,而且具有较少的时间开销和通信开销,并通过动态匿名机制保护车辆的身份和位置隐私.

关键词 车载自组网;合谋 Sybil 攻击;隐私保护;时间戳标识;动态匿名机制

中图法分类号 TP393 **DOI 号** 10.11897/SP.J.1016.2018.02148

Spatio-Temporal Analysis Based Resist Conspiracy Sybil Attack Detection in VANETs

SHI Ya-Li WANG Liang-Min

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

Abstract In Vehicular Ad Hoc Networks (VANETs), Attacker can obtain multiple network identities by forging, stealing and conspiring with other legal vehicles, then they use these Sybil identities to transmit fake traffic information to create an illusion traffic congestion, even would cause more serious traffic accidents. The most current Sybil attack detection scheme primarily detects forged identity and stolen identity Sybil attack, there is rare research to detect conspiracy Sybil attack. In addition, Sybil attack detection need to bind each vehicle to a single identity in order to keep adversaries from playing multiple roles or spoofing with other legitimate identities, this will lead to privacy reveal issues. In order to balanced solve the two conflicting problems between Sybil attack detection and privacy protection, we propose a resist conspiracy Sybil attack detection method based on Spatio-Temporal Analysis based Resist Conspiracy Sybil Attack (STARCS). The method uses anonymous road side unit (RSU) released timestamp token as identity in VANETs, and there set a table to record RSU that last passed and timestamp by Trust Authority (TA), the table is called request information table to record the RSU and timestamp

收稿日期:2016-12-04;在线出版日期:2017-04-19.本课题得到国家自然科学基金(61472001)和江苏省重点研发计划项目(BE2015136)资助.**石亚丽**,女,1992 年生,硕士研究生,主要研究方向为车联网安全.E-mail: shiyali92@163.com. **王良民**,男,1977 生,博士,教授,博士生导师,主要研究领域为物联网信息处理技术、物联网安全协议、车联网安全结构等.

which vehicle last passed, to defend the generation of stolen and conspired Sybil identities. In this paper, each alarm event only allows each vehicle to release an alert message with timestamp token to detect Sybil attack, and we check whether the timestamp token contained in multiple alert messages and used by a plurality of vehicles at the same time to detect conspiracy Sybil attack which attacker and conspired vehicles using the same identity at the same time, and based on the adjacent relation tag of RSUs which embedded in the timestamp token to detect conspiracy Sybil attack which attacker conspired with the long-distance vehicles launch Sybil attack. Due to we detect conspiracy Sybil attack from the perspective of time to analyze whether the identity is abused or not and from the perspective of spatial to analyze whether the identity is appearing unreasonable displacement or not, that is, from the spatio-temporal analysis to resist and detect conspiracy Sybil attack. Theoretical analysis and simulation results show this method not only can defend or detect various types of Sybil attack, but also has less computation overhead and communication overhead, and it can protect the privacy of vehicle's identity and position by dynamic anonymity mechanism.

Keywords　VANETs; conspiracy Sybil attack; privacy protection; timestamp token; dynamic anonymous mechanism

1　引　言

在车载自组网(Vehicular Ad hoc Networks, VANETs)中,车辆主要通过车辆之间(Vehicular to Vehicular, V2V)或车辆与基础设施(Vehicular to Infrastructure, V2I)的通信,将感知的道路信息(如道路拥堵、碰撞事故等)发送给附近车辆,实现道路信息的及时共享,从而避免潜在的事故发生,增强交通道路安全[1]. 同时,VANETs 通过车辆之间的交互通信提供大量应用,如碰撞警报、电子刹车灯、提供最佳行车路线等,从而促进交通管理,提高人们的出行质量[2]. 然而,由于 VANETs 本身具有无线多跳的通信方式、动态变化的拓扑结构及车辆运行受道路环境的限制等特点[3],使得其安全问题日益突出,成为 VANETs 研究的重点之一.

在众多安全问题中,攻击者利用获得的多个身份向周围车辆发送虚假的交通信息,会影响网络的正常运行,损害 VANETs 应用所带来的效益,甚至引发更严重的交通事故,这种攻击行为被称为 Sybil 攻击. Sybil 攻击最初由 Douceur[4] 在 P2P 网络中提出的,是指攻击者非法拥有多个身份,并利用这些身份来攻击其他实体. 研究发现 Sybil 攻击在 VANETs 中也具有严重的威胁,如攻击者利用多个身份发送虚假信息,伪造拥堵的交通场景,影响其他车辆的正常行驶[5-6];由于 VANETs 中存在许多机制需要车辆之间的相互协作,攻击者可以利用多个 Sybil 身份破坏网络协议[4],如路由协议、资源分配机制和恶意行为检测机制等. 另外,攻击者还可以借助 Sybil 身份发动其他类型的攻击[3,7],如 DOS 攻击、黑洞攻击以及虫洞攻击等. 为此,检测 Sybil 攻击对 VANETs 发展至关重要.

目前在 VANETs 中,研究者提出的 Sybil 攻击检测方案,主要有基于资源检测[4,8]、基于车辆滥用假名[9]、基于位置验证[10-11]、基于身份认证[12-16]等方案. 基于资源检测的方案[4,8]无法抵抗具有较多资源的攻击者;基于车辆滥用假名的检测方法[9]主要依赖于每个车辆具有相同的粗细粒度哈希值,通过网络中多个假名具有同一细粒度哈希值来检测车辆滥用假名的行为,但该方法无法检测出偷窃身份和合谋身份的 Sybil 攻击;基于位置验证的方案[10-11]通过位置验证方法检测车辆是否位于其声称的位置发现 Sybil 攻击行为,该方法依赖硬件的支持;现有的 Sybil 攻击检测方案大多基于身份认证的检测[12-16]. 其中方案[12-13]依据时间戳序列检测 Sybil 攻击;方案[14]通过对比不同车辆轨迹的相似性检测 Sybil 攻击;文献[15-16]中车辆利用 BRSU 发布的标记检测 Sybil 攻击,但该方法 BRSU 被攻击将无法为车辆提供标记,其范围内的车辆将无法发送消息.

以上这些检测方案只考虑攻击者独自发动 Sybil 攻击的行为,如攻击者通过伪造或偷窃的方式

获得多个 Sybil 身份，没有考虑存在攻击者与其他车辆合谋的情况(在此只考虑其他车辆将身份提供给攻击者的行为).攻击者通过利用合谋车辆的身份获得多个 Sybil 身份发动 Sybil 攻击行为，但由于这些 Sybil 身份是合谋车辆的合法身份，使得现有的检测方案很难检测出合谋 Sybil 攻击.另外，检测 Sybil 攻击需要确保车辆实体在网络通信时仅绑定一个网络身份以防止攻击者扮演多个身份来欺骗其它车辆，否则，这种做法会造成车辆隐私的泄露.VANETs 中的隐私通常包含身份隐私、服务信息隐私和位置隐私.身份隐私，即车辆及车辆用户的真实身份信息，如驾驶证号、车主身份证等.位置隐私即需要保护车辆的地理位置和路径轨迹不泄露.为此，在检测 Sybil 攻击时需要满足以下两点：(1)车辆的匿名性.恶意车辆无法通过车辆的假名信息获取车辆的真实身份；(2)车辆的位置隐私.车辆的位置信息往往包含车主的重要隐私，如车辆停留在整容医院，攻击者通过车辆位置推断车主隐私.为此，本文提出了一种基于时空分析的抗合谋 Sybil 攻击检测方法，该方法利用匿名 RSU 发布的时间戳标记作为车辆在 RSU 区域内的身份，通过为网络中设置请求信息表抵御伪造 Sybil 身份和合谋 Sybil 身份的产生，根据警报信息中包含的标识是否被多个车辆同时使用检测攻击者与合谋车辆同时使用同一身份的合谋 Sybil 攻击，并根据标识中嵌入的 RSU 位置关系标签检测车辆出现不合理位移的合谋 Sybil 攻击，由于从时间上身份是否被滥用和空间上身份是否出现不合理位移的情况来检测合谋 Sybil 攻击，即从时空关系上分析是否存在合谋 Sybil 攻击.本文的主要贡献在于：

(1)TA 设置请求信息表抵御伪造 Sybil 身份和合谋 Sybil 身份的产生.

(2)车辆利用动态匿名方法向 RSU 请求时间戳标识保护车辆的身份隐私，RSU 采用动态匿名机制防止恶意车辆根据 RSU 的位置追踪车辆的位置和行驶轨迹.

(3)根据标识中嵌入的 RSU 位置关系标签检测出现不合理位移的合谋 Sybil 攻击.

2 相关工作

Sybil 攻击最早由 Douceur[4] 在 P2P 网络中提出，并提出了资源测试的检测方法.该方法假设网络中的所有节点都拥有相同且有限的资源(如计算资源、存储资源和通信资源等)，通过验证网络中的某个身份对应的实体是否具有独立实体应当具有的能力来检测出 Sybil 节点.例如，假设网络中所有节点的计算能力相同且有限，验证节点向被验证节点发送计算难题，由于 Sybil 节点将资源分配给其虚假身份，则该节点将不能按照规定的时间计算出难题的正确答案，从而检测出 Sybil 节点.但这种方法需要同时验证多个节点，否则攻击者可以分时利用自己的资源导致检测失效.同时该方法并不适用于 VANETs，因为计算速度和存储能力不是车联网的瓶颈问题，而通信测试会造成额外的通信开销；Newsome 等人[8] 提出无线资源测试的方法，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，从而限制节点一次只能以一个身份发送消息.但这些方法并不适用于 VANETs，因为车辆能够轻易获得这些资源.

Zhou 等人[9] 提出一种假名分配机制 P2DAP 来防止恶意车辆滥用假名，该方法中 DMV 给每个车辆分配一个匿名池，利用粗粒度密钥 K_c 和细粒度密钥 K_f 依次对车辆的假名进行计算得到车辆假名的粗粒度哈希值和细粒度哈希值，由于 RSU 已知粗粒度密钥 K_c，可以验证接收消息的车辆假名，若 RSU 检测到多个假名的粗粒度哈希值相同，则将这些假名发送给 DMV 计算假名的细粒度哈希值，多个节点的细粒度哈希值相同即被认为存在 Sybil 攻击.

由于一个实体车辆只具有一个相对精确的位置，故一个车辆身份对应一个位置，基于这种思想，Yu 等人[10] 利用预设的无线信号传播模型和收到的信号强度(Received Signal Strength Indication，RSSI)分布模型计算邻居节点的估计位置，如果估计位置与其发送的数据包中的位置信息不相符，那么该节点是 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 节点.然而，这种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自组网中可能并不实用.Jin 等人[11] 提出基于物理测量的 Sybil 节点检测机制，利用传输信息的物理测量值检测 Sybil 攻击，利用信息到达时差技术对信息源进行定位，通过比较信息中包含的位置与所定位的位置是否相同检测 Sybil 攻击.

根据车辆的动态移动特性，任何两个车辆在长时间内总是同时经过相同的 RSU 是小概率事件，且一辆车也不会同时出现在不同的 RSU 处.基于

这种思想，Park 等人[12-13]提出一种基于时间戳序列抵御 Sybil 攻击的方法，利用 RSU 为合法车辆发布时间戳证书，由于两个车辆不会同时经过多个相同的 RSU，若存在两条信息具有相似的时间戳序列则被认为存在 Sybil 攻击. 但由于方案[12,13]中 RSU 发布的时间戳是广播发送的，恶意车辆可以窃听其它车辆的时间戳. 而 Footprint[14]中车辆主动向 RSU 请求时间戳签名，并利用这些签名形成轨迹，通过比较所有邻居车辆轨迹相似性检测 Sybil 节点. 为了保护车辆的位置隐私，RSU 发送数字签名时采用环签名机制实现了模糊签名和签名的短链接性，保护了车辆的位置隐私和路径信息. 但该方案允许车辆经过 RSU 时可以获取多个带有时间戳的数字签名，所以容易被攻击者利用发动 Sybil 攻击，该方法也无法抵御合谋 Sybil 攻击. 本文的方法最接近方案[15-16]，Hussain 等人[15-16]利用 RSU 发布的身份标记来检测 Sybil 攻击，由于车辆在发送警报事件时每个身份标记只能用于发送一次警报事件的信息，RSU 通过收集警报事件的信息并检测多个事件信息是否包含同一身份标记检测 Sybil 攻击.

综上所述，当前各类研究方法均具有各自的特点，表 1 对相关工作进行了对比分析. 其中，✓表示能够实现对应的需求，* 表示不能完成对应的需求，△表示没有考虑对应的要求. 从表中可以看出，没有那种检测方法主要针对合谋 Sybil 攻击进行研究. 为此，本文提出一种基于时空分析的抗合谋 Sybil 攻击检测方法，该方法不仅能够抵御或检测合谋 Sybil 攻击，也能够抵御潜在 Sybil 攻击的发生，保护车辆的身份隐私和行驶轨迹隐私，且具有较少的时间开销和通信开销.

表 1　各方案的性能比较

检测方法	伪造 Sybil 身份	偷窃 Sybil 身份	合谋 Sybil 身份	身份隐私	位置隐私	RSU 支持	完整性
基于资源检测[4,8]	✓	*	*	△	△	*	△
基于滥用假名[9]	✓	*	*	✓	✓	✓	△
基于位置验证[10,11]	✓	✓	△	△	*	*	△
基于时间戳序列[12,13]	✓	✓	*	✓	*	✓	*
基于行驶轨迹[14]	✓	✓	*	✓	✓	✓	✓
基于标记[15,16]	✓	✓	*	✓	*	✓	✓
STARCS	✓	✓	✓	✓	✓	✓	✓

3　模型与目标

3.1　系统模型与假设

本文采用分层的 VANETs 系统模型，如图 1 所示，主要实体包括可信机构 TA(Trust Authority)、路边基础设施 RSU(Road-Side Units)、车载单元 OBU(On-Board Units). 模型中各实体的功能如下：

(1) TA 负责为 VANETs 中的车辆和 RSU 发布密钥和系统参数. TA 设置请求信息表来记录车辆向经过的 RSU 发送身份请求时经过的 RSU 和请求时间戳，用于验证请求车辆行为的合法性. TA 根据 RSU 的位置结构，为每个 RSU 设置一个位置关系标签. 在新的 RSU 加入 VANETs 或者有 RSU 因损坏等原因被 VANETs 删除时，TA 会更新 RSU 的位置关系标签. 为了防止 RSU 位置的泄露，每经过一段时间，TA 也会重新更新 RSU 的标签.

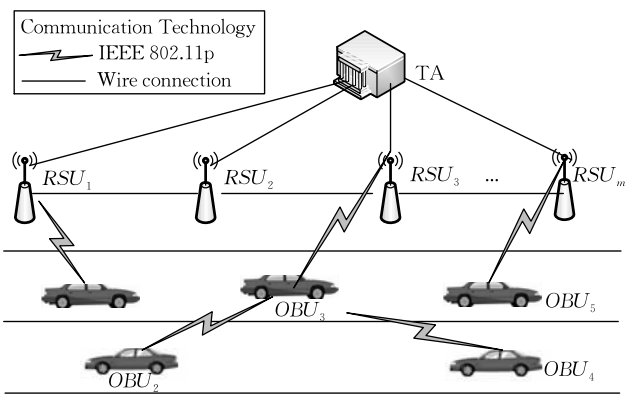


图 1　VANETs 的系统模型

(2) RSU 合理部署于所在城市(如十字路口、停车场入口等[14])，可以通过无线的方式与车辆通信，也可以通过有线方式与其它 RSU 或 TA 通信. 根据 DSRC 标准①②，RSU 的通信范围要远大于车辆的通信范围，故 RSU 可以定期向其通信范围内的合法车辆广播身份信息和位置关系标签，并为路过的合法车辆提供时间戳标识.

(3) 车辆除了配备 OBU 之外，还配备 GPS 接收设备和短距离通信模块(如 DSRC)，车辆能够通过 V2V 和 V2I 与其它车辆或其它 RSU 进行通信.

① Dedicated short range communications (DSRC). http://www.etsi.org/index.php/Technologies-clusters/technologies/intelligent-transport/dsrc

② Dedicated short range communications (DSRC). http://www.dsrc.com

本文遵循以下安全假设：

假设 1. TA 总是在线，完全可信且不会被攻击者攻破.

假设 2. RSU 也是可信的，RSU 之间是时间同步的.

假设 3. RSU 通过有线与 TA 或其它 RSU 通信，使得 RSU 之间的时间同步很容易实现.

3.2 预备知识

椭圆曲线是一个二元方程解的集合. 椭圆曲线密码体制中使用的椭圆曲线在有限域 F_q 上，其具体的表现形式为 $E_q(a,b)$：$y^2=x^3+ax+b(\mathrm{mod}\,q)$，其中，$a,b\in E_q$，$q>3$，且 $4a^3+27b^2\neq 0(\mathrm{mod}\,q)$. $E(F_q)$表示椭圆曲线 $E_q(a,b)$上的点和一个无穷远点 O 构成一个加法群. 椭圆曲线上存在离散对数难题(Elliptic Curve Discrete Logarithm Problem，ECDLP)[17].

定义 1. 椭圆曲线离散对数难题(Elliptic Curve Discrete Logarithm Problem，ECDLP). 假设 G 是 $E(F_q)$中一个阶为 q 的加法子群，P 和 Q 是椭圆曲线 $E_q(a,b)$上的两点，寻找一个 $x\in Z_q^*$，使得 $x\cdot P=Q$ 成立.

3.3 攻击模型

Sybil 攻击是一种内部攻击，可以主动且理性地发起攻击[16]. 攻击者在 VANETs 中拥有合法的身份，且只攻击自己感兴趣的车辆或者获取感兴趣的网络资源. 另外，攻击者可以主动窃听无线信道中传播的信息，通过窃取其它车辆的身份获得 Sybil 身份.

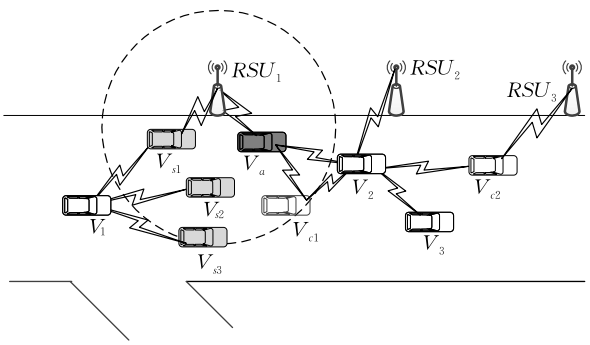


图 2 合谋 Sybil 攻击场景

攻击者也可以通过与其它车辆合谋的方式获取多个合谋 Sybil 身份(合谋车辆提供给攻击者的合法的身份)，本文主要考虑以下 2 种情况：(1) 合谋车辆将自己正在使用的身份发送给攻击者使用；(2) 合谋车辆将请求信息发送给攻击者，由攻击者自己更新得到合谋 Sybil 身份.

由于这些合谋 Sybil 身份是由合谋车辆提供的合法身份，检测方案很难检测出这种攻击行为. 如图 2 所示，假设攻击者为 V_a，合谋车辆为 V_c，Sybil 节点为 V_s，合法的车辆为 V_i. 每种合谋的场景描述如下：(1) 合谋车辆 V_{c1} 和 V_{c2} 主动将自己正在使用的身份发送给攻击者 V_a，攻击者通过这种方式获取多个身份发送虚假警报信息(如前方拥堵)，后方车辆(假设为车辆 V_1)接收到虚假信息后，会选择其它道路行驶. 由于 V_{c1} 和 V_{c2} 的身份是合法的，车辆 V_1 很难检测发送的警报信息是多个不同车辆发送，还是同一车辆的多个 Sybil 身份发送；(2) 远距离的合谋车辆 V_{c2} 获取身份后，将请求信息及临时的私钥发送给攻击者 V_a，由攻击者向 RSU_1 发送请求信息获取时间戳标识，攻击者通过这种方式获取多个身份向附近车辆发送虚假交通信息(如前方道路正在施工，但攻击者发送道路流畅)，后方车辆(假设为车辆 V_1)继续行驶，会在施工处形成严重的拥堵. 由于攻击者发送的请求信息中的请求者实际上是合谋车辆，RSU 很难验证请求信息是否合法或者重用.

3.4 设计目标

针对 Sybil 攻击给 VANETs 带来的危害以及现有的 Sybil 攻击检测方案存在的不足，本文提出了基于时空分析的抗合谋 Sybil 攻击检测方法. 该方法的设计目标有：

(1) 节点独立检测. Sybil 攻击是利用多个身份协作破坏网络的正常运行，为了消除检测方案中存在潜在 Sybil 攻击的可能，方案需要独立地实施检测.

(2) 隐私保护. 在检测 Sybil 攻击时，需要保护车辆的真实身份不被泄露. 由于车辆的位置信息是用户隐私的重要部分，检测方案也需要保护车辆的位置信息和运行轨迹.

(3) 在线检测. 当网络中有恶意车辆发动 Sybil 攻击时，需要及时地检测出 Sybil 攻击防止恶意车辆实现它的意图.

(4) 抵御潜在 Sybil 攻击. 攻击者发动 Sybil 攻击需要获取多个身份，Sybil 身份可以通过伪造、偷窃以及与其它车辆合谋等方式获取. 抵御 Sybil 节点的产生，可以抵御潜在的 Sybil 攻击的发生.

(5) 检测合谋 Sybil 攻击. 攻击者通过利用多个与其合谋的车辆身份发动 Sybil 攻击，文中只考虑合谋车辆将合法身份提供给攻击者的情况. 方案需要能够检测同一 RSU 区域内的合谋车辆的身份是否被攻击者使用，或者远距离车辆是否将合法身份

提供给攻击者使用.

4　STARCS 方法

本方法主要包含 3 个阶段：(1) 系统初始化；(2) 区域身份获取；(3) Sybil 攻击检测. 文中使用的主要参数如表 2 所示.

表 2　符号注释表

字母	含义
sk	TA 的私钥
PK	TA 的公钥
sk_{R_j}	RSU j 的私钥 $sk_{R_j}=(sk_{R_j}^1, sk_{R_j}^2)$
PK_{R_j}	RSU j 的临时公钥
RID_{R_j}	RSU j 的真实身份
PID_{R_j}	RSU j 的假名 $PID_{R_j}=(PID_{R_j}^1, PID_{R_j}^2)$
L_{R_j}	RSU j 的位置关系标签
sk_i	车辆 i 的私钥 $sk_i=(sk_i^1, sk_i^2)$
PK_i	车辆 i 的公钥
RID_i	车辆 i 的真实身份
PID_i	车辆 i 的假名 $PID_i=(PID_i^1, PID_i^2)$
$h(\cdot)$	无碰撞单向哈希函数 $h:\{0,1\}^* \to Z_q^*$
$H(\cdot)$	映射到点的哈希函数 $H:\{0,1\}^* \to G$
$\|$	消息的连接操作符
$\oplus$	抑或操作符

4.1　系统初始化

在初始化过程中，TA 负责为 VANETs 中所有实体初始化. 根据 IEEE 标准，每个车辆和 RSU 装有防篡改设备，攻击者无法获取设备里存储的信息.

(1) TA 初始化

① 根据双线性 $(P, q, \mathbb{G}_1, \mathbb{G}_2, e)$，TA 选择 2 个随机数字 $s, s_1 \in Z_p^*$，s 为 TA 的私钥；

② TA 选择一个随机数集合 $\Gamma_j \subset Z_p^*$，其中，$\Gamma_j=\{t_{j1}, t_{j2}, \cdots, t_{jk}, \cdots, t_{jn}\}$；

③ TA 计算 $PK=s \cdot P$，$PK_{R_j}=t_j \oplus RID_{R_j}$，$PK_1=s_1 \cdot P$，$sk_i^1=s \cdot H(RID_i)$；

④ TA 根据 RSU 的位置结构产生 RSU 标签 $\boldsymbol{L}_R$，标签 $\boldsymbol{L}_R=\{l_1, l_2, \cdots, l_n\}$ 是一维矩阵，其中，当前 RSU 值为 1，邻居 RSU 值为 −1，非邻居 RSU 值为 0.

(2) RSU 初始化

① RSU_j 下载临时公钥 PK_{R_j} 集，s_1 和 RSU_j 的位置关系标签 L_{R_j}；

② RSU_j 选择随机数 $r_j \in Z_p^*$；

③ RSU_j 计算 $PID_{R_j}^1=r_j \cdot P$，$PID_{R_j}^2=PK_{R_j} \oplus H(r_j \cdot PK)$；

④ RSU_j 计算 $sk_{R_j}^1=s_1 \cdot PID_{R_j}^1$，$sk_{R_j}^2=s_1 \cdot H(PID_{R_j}^1 \| PID_{R_j}^2)$.

(3) OBU 初始化

① V_i 下载部分私钥 sk_i^1；

② V_i 选择随机数 $r_i \in Z_p^*$ 作为 sk_i^2；

③ V_i 计算 $PK_i=r_i \cdot P$；

④ V_i 计算 $PID_i^1=r_i \cdot H(RID_i)$，$PID_i^2=RID_i \oplus H(r_i \cdot PK)$.

4.2　方案总体介绍

本文主要针对道路上发生警报事件时，车辆向附近车辆发送警报消息的场景，方案主要检测此场景中是否存在 Sybil 攻击. 图 3 为基于时空分析的抗合谋 Sybil 攻击检测的流程图.

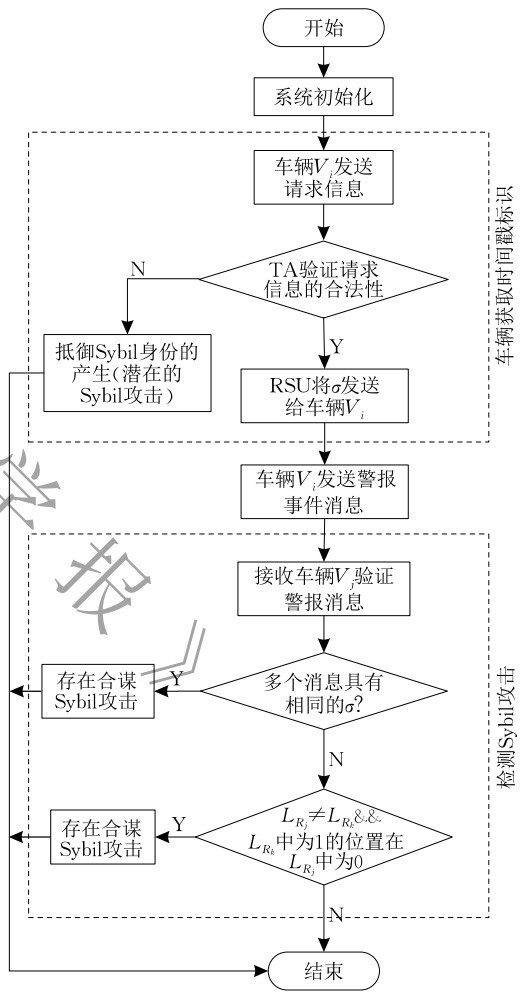


图 3　基于时空分析的抗合谋 Sybil 攻击检测的流程图

车辆完成初始化后，需要向经过的 RSU 请求时间戳标识作为车辆在该区域内的唯一通信身份. 当车辆进入 RSU 的通信范围，车辆选择临时公钥和假名生成请求信息，并主动向 RSU 发送请求信息. 由于 RSU 无法直接验证车辆的合法性，故将请求信息发送给 TA 来验证请求车辆身份的合法性和行为的合法性. 由表 3 所示，TA 设置请求信息表用

于记录每个合法车辆前一次经过的 RSU 和时间戳(请求信息表在每个合法车辆注册后都会在请求信息表中记录合法车辆的真实身份). TA 通过计算请求车辆和 RSU 的真实身份,从而避免外部攻击者获取 RSU 的时间戳标识或内部攻击者在某个 RSU 处获取多个时间戳标识. 另通过与上一次经过的 RSU 的比较,防止攻击者利用合谋车辆的请求信息企图获取时间戳标识. TA 验证请求信息的合法性,保证请求车辆经过每个 RSU 时有且仅能获取一个时间戳标识,抵御潜在的 Sybil 攻击.

表 3 请求信息表

车辆(RID_i)	RSU(RID_{R_j})	时间戳(T_i)

当发生警报事件时,车辆发送的警报消息中都包含时间戳标识,接受车辆通过验证时间戳标识的合法性检测伪造 Sybil 攻击,根据同一警报事件的多个消息中是否具有相同的时间戳标识来检测攻击者与合谋车辆同时使用同一身份的合谋 Sybil 攻击;并根据标识中嵌入的 RSU 位置关系标签和当前请求的 RSU 位置关系标签检测出现不合理位移的合谋 Sybil 攻击.

4.3 获取时间戳标识

车辆主要通过两种方式获取时间戳标识[14]:(1) RSU 通过定期广播的方式向经过的车辆发送时间戳标识;(2) 车辆主动向经过的 RSU 发送请求信息以获取时间戳标识. 但由于车载自组网是一种无线网络,攻击者容易从无线信道中窃听 RSU 发布的时间戳标识,并且定期广播的方式不具备安全性,故本文采用车辆主动向 RSU 请求时间戳标识的方式.

本文由 TA 设置请求信息表用于验证请求车辆行为的合法性,保证车辆通信时有且仅有一个区域身份标识,防止外部攻击者获取时间戳标识或内部攻击者在 RSU 处获取多个时间戳标记,从而抵御攻击者产生 Sybil 身份. 车辆和 RSU 都采用动态假名机制,防止攻击者追踪车辆的真实身份,车辆每进入新的 RSU 范围都会选择新的临时公钥和假名与其它实体进行通信. 为防止攻击者通过 RSU 的位置追踪车辆的行驶轨迹,本文将时间分成多个片段,当前时间表示为 $t_k \in [t_k, t_{k+1})$,每个时间片内 RSU 动态改变自己的公钥和假名,并向其通信范围内的车辆广播身份信息.

车辆进入 RSU 通信范围会主动请求时间戳标识,图 4 为车辆请求时间戳标识的过程,具体过程如下:

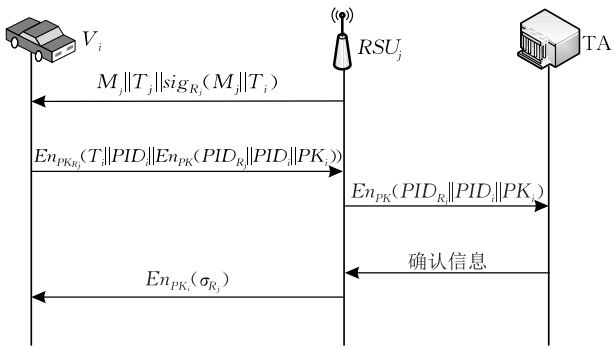


图 4 车辆请求时间戳标识的过程

步骤 1. RSU_j 定期广播包含自身临时公钥和假名的身份消息 Bea 以供其通信范围内车辆对其验证,消息内容为

$$\begin{cases} Bea = (M_j \parallel T_j \parallel sig_{R_j}(M_j \parallel T_j)) \\ M_j = PID_{R_j} \parallel PK_{R_j} \parallel sig_{\mathrm{TA}}(PK_{R_j}) \end{cases} \tag{1}$$

其中,PK_{R_j},PID_{R_j} 分别是 RSU_j 的临时公钥和假名,$sig_{\mathrm{TA}}(PK_{R_j})$ 为 TA 对 RSU_j 的临时公钥的签名,T_j 为身份消息 Bea 的时间戳. Sig 表示 ECDSA (Elliptic Curve Digital Signature Algorithm)签名.

步骤 2. RSU_j 通信范围内的车辆 V_i 收到 RSU_j 的身份消息 Bea 之后,根据如下步骤对 RSU_j 的身份进行验证:

(1) 车辆 V_i 首先检查 RSU_j 身份消息 Bea 的新鲜性以防止重放攻击. 车辆检查不等式(2)是否成立,若不等式成立,车辆 V_i 继续验证,否则车辆 V_i 丢弃该身份消息;

$$\Delta T \geq T' - T_j \tag{2}$$

其中,ΔT 是系统设置的最大传输时延. T' 为车辆 V_i 收到身份信息 Bea 的时刻.

(2) 车辆 V_i 利用 TA 的公钥验证 RSU_j 的临时公钥的合法性,若式(3)成立,则说明 RSU_j 的公钥是 TA 发布的,否则直接丢弃该身份消息;

$$Verf(sig_{\mathrm{TA}}(PK_{R_j}), PK) = PK_{R_j} \tag{3}$$

(3) 车辆 V_i 利用 RSU_j 的临时公钥验证 RSU_j 签名,若式(4)成立,则 RSU_j 的身份消息 Bea 为合法的身份信息,否则丢弃该身份消息,并等待 RSU 发送新的身份消息 Bea;

$$Verf(sig_{R_j}(M_j \parallel T_j), PK_{R_j}) = M_j \parallel T_j \tag{4}$$

步骤 3. 车辆 V_i 生成请求信息 $M_i^{t_k}$,并主动向 RSU_j 发送请求信息请求时间戳标识,请求信息格式为

$$M_i^{t_k} = En_{PK_{R_j}}(T_i \| PID_i \| En_{PK}(PID_{R_j} \| PID_i \| PK_i)) \tag{5}$$

其中 T_i 为请求信息的时间戳，PK_i，PID_i 为请求车辆 V_i 的临时公钥和假名，PID_{R_j} 为 RSU_j 的假名，E_n 代表 ECIES(Elliptic Curve Integrated Encryption Scheme)加密.

步骤 4. RSU_j 接收到车辆 V_i 的请求信息后，首先将请求信息解密，再验证其新鲜性，计算不等式(6)是否成立，若不等式成立，将请求信息发送给 TA 验证，否则 RSU_j 丢弃该请求消息；

$$\Delta T \geq T' - T_i \tag{6}$$

其中，T' 为 RSU_j 收到请求信息的时刻，ΔT 是系统设置的最大传输时延.

步骤 5. TA 接收到请求信息，首先验证请求车辆身份的合法性，由式(7)得到车辆 V_i 的真实身份，若请求车辆不在请求信息表中，则该车辆为恶意车辆；否则验证请求车辆行为的合法性，由式(8)得到 RSU_j 的真实身份，若 RSU_j 和请求信息表中车辆前一次经过的 RSU_k 相同，且请求时间间隔在同一时间片 Δt 内，说明该车辆企图在 RSU_j 处获得多个时间戳标识；若 RSU_j 和请求信息表中车辆前一次经过的 RSU_k 不同且不相邻，即该车辆出现不合理位移，认为该车辆企图利用其它车辆的请求信息获得多个 Sybil 身份；否则将 RSU_j 和请求时间戳 T_i 存储在请求信息表中.

$$\begin{aligned} RID_i &= PID_i^2 \oplus H_1(PK_i \cdot s) \\ &= RID_i \oplus H_1(r_i \cdot PK) \oplus H_1(PK_i \cdot s) \\ &= RID_i \end{aligned} \tag{7}$$

$$\begin{aligned} RID_{R_j} &= PID_{R_j}^2 \oplus t_j \oplus H(PID_{R_j}^1 \cdot s) \\ &= t_j \oplus RID_{R_j} \oplus H(r_j \cdot PK) \oplus t_j \oplus H(PID_{R_j}^1 \cdot s) \\ &= t_j \oplus RID_{R_j} \oplus H(r_j \cdot s \cdot P) \oplus t_j \oplus H(r_j \cdot P \cdot s) \\ &= RID_{R_j} \end{aligned} \tag{8}$$

步骤 6. 请求信息通过 TA 验证后，向 RSU_j 发送确认信息，RSU_j 接收到 TA 的反馈信息后，根据式(9)生成时间戳标识 σ_{R_j}，并利用车辆的临时公钥对其加密后发送给请求车辆.

$$\sigma_{R_j} = sk_{R_j}^1 + h(M')sk_{R_j}^2 \tag{9}$$

其中，M' 包含请求时间戳 t_{R_j}，当前 RSU 位置关系标签 L_{R_j}.

4.4 Sybil 攻击检测

当发生警报事件时，车辆向附近车辆发送警报消息，接收车辆需要通过验证事件消息中包含的时间戳标识检测是否存在 Sybil 攻击. 车辆检测 Sybil 攻击的过程如图 5 所示. 具体过程如下：

步骤 1. 当发生警报事件时，车辆 V_i 将警报消息 M_k^i 及消息签名一起发送给附近车辆(假设为车辆 V_j)，M_k^i 格式为

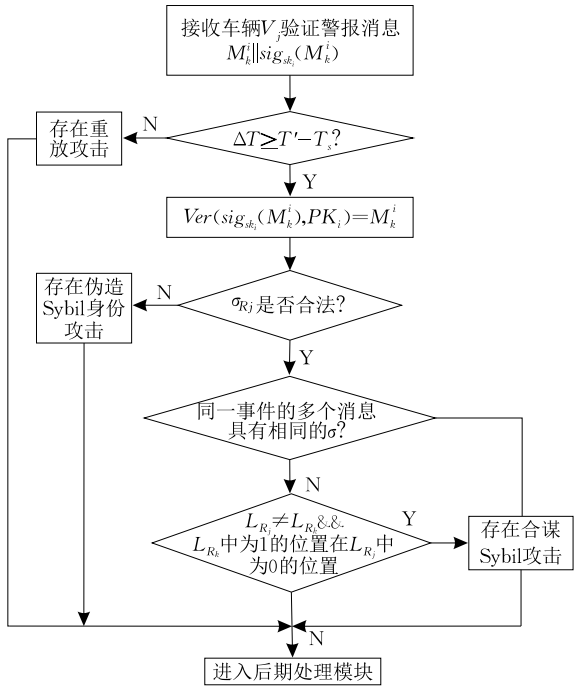


图 5　检测 Sybil 攻击流程图

$$M_k^i = (T_s, PK_i, PID_i, PID_{R_j}, EI_k, \sigma_{R_j}) \tag{10}$$

其中，PK_i，PID_i 表示车辆的临时公钥和假名，PID_{R_j} 表示 RSU_j 的假名，T_s 为消息的时间戳，EI_k 为警报事件的内容，σ_{R_j} 为从 RSU_j 处获得的时间戳标识.

步骤 2. 车辆 V_j 接收到警报消息后，首先判断消息的新鲜性，再根据式(11)验证发送车辆的签名. 如果通过验证，则进行 Sybil 攻击检测，否则丢弃消息；

$$Ver(sig_{sk_i}(M_k^i), PK_i) = M_k^i \tag{11}$$

步骤 3. 车辆 V_j 首先根据式(12)验证时间戳标识的合法性，若验证无法通过，则说明时间戳标识是恶意伪造的，发送车辆为 Sybil 节点；否则检测同一警报事件的多个警报信息中是否存在相同的时间戳标识，若存在，说明攻击者利用其时间戳标识发送多个警报事件的信息或者攻击者和合谋车辆同时使用同一时间戳标识发送警报事件的信息；否则根据时间戳标识中嵌入的 RSU 位置关系标签 L_{R_j} 检测是否存在车辆发生不合理位移的合谋 Sybil 攻击. 计算不等式(13)，若不等式成立，说明车辆出现不合理位移，则认为存在攻击者与其它车辆发动合谋 Sybil 攻击.

$$e(\sigma_{R_j}, P) = e(PID_{R_j}^1 + h(M')H(PID_{R_j}^1 \| PID_{R_j}^2), PK_1) \tag{12}$$

$$L_{R_j} \neq L_{R_k} \tag{13}$$

其中，L_{R_j} 表示发送车辆所在的 RSU 位置关系标签，L_{R_k} 表示接收车辆所在的 RSU 位置关系标签，当等式(13)不成立时，说明发送车辆和接收车辆不在同一个 RSU 范围内. 此时，若 L_{R_k} 标签中为 1 的位置在 L_{R_j} 标签中为 0，表示发送车辆与接收车辆的所在 RSU 不相邻，发送车辆是远距离的车辆，这说明存在攻击者利用远距离的车辆的身份发动 Sybil 攻击.

5 协议安全性分析

本节主要从抗重放攻击、抵御 Sybil 攻击、检测 Sybil 攻击、匿名性和不可追溯性及条件隐私保护这 5 个方面来分析 STARCS 方法的安全性.

(1)抗重放攻击. 为了确保信息的新鲜性，文中在发送警报信息时会加入时间戳，当车辆接收到警报信息后，通过验证时间戳来防止攻击者发动重放攻击. 假设 T_s 表示消息的时间戳，T_r 表示接收到消息的时间，ΔT 表示系统设置的最大传输时延. 当车辆接收到消息后，接收车辆首先通过式(14)检查消息是否过期. 如果消息中的时间戳 T_s 过期，则丢弃这个消息. 同样，车辆的请求信息中包含时间戳，从而防止攻击者利用请求信息多次向 RSU 请求时间戳标识.

$$\Delta T \geq T_r - T_s \tag{14}$$

(2)抵御 Sybil 攻击. 在 STARCS 中，RSU 在发布时间戳标识时利用请求车辆的临时公钥对时间戳标识进行加密. 根据 DH 计算问题的困难性，攻击者无法通过临时公钥或假名计算出发送车辆的发送车辆的私钥，防止攻击者拦截其它车辆的时间戳标识，从而抵御攻击者偷窃合法车辆的身份. 另外，TA 设置请求信息表存储合法车辆前一次经过的 RSU 和请求时间戳，由于 TA 根据式(7)、(8)能够计算出请求车辆 V_i 的真实身份 RID_i 和 RSU_j 的真实身份 RID_{R_j}，根据式(15)、(16)判断请求车辆是否在短时间内向同一 RSU 多次请求时间戳标识，抵御攻击者获取多个 Sybil 身份.

$$L_{R_j} = L_{R_k} \tag{15}$$

$$t_{R_j} - t_{R_{j-1}} \leq \Delta t \tag{16}$$

方案考虑到攻击者会与其它车辆合谋的情况，攻击者利用其它车辆的请求信息向 RSU 请求时间戳标识. 由于方案为每个 RSU 设置位置关系标签 L_{R_j}，TA 在验证请求信息时，确定请求车辆两次经过的 RSU 位置关系，根据请求车辆两次经过的 RSU 位置的合理性，TA 检测出请求车辆出现不合理位移，抵制攻击者与远距离的其它车辆合谋获得 Sybil 身份的攻击.

(3)检测 Sybil 攻击. 在 STARCS 中，车辆根据警报消息中包含的时间戳标识检测 Sybil 攻击. 车辆在接收到警报消息后，根据以下公式判断时间戳标识的合法性，若等式不成立，则说明攻击者伪造 Sybil 身份发动 Sybil 攻击.

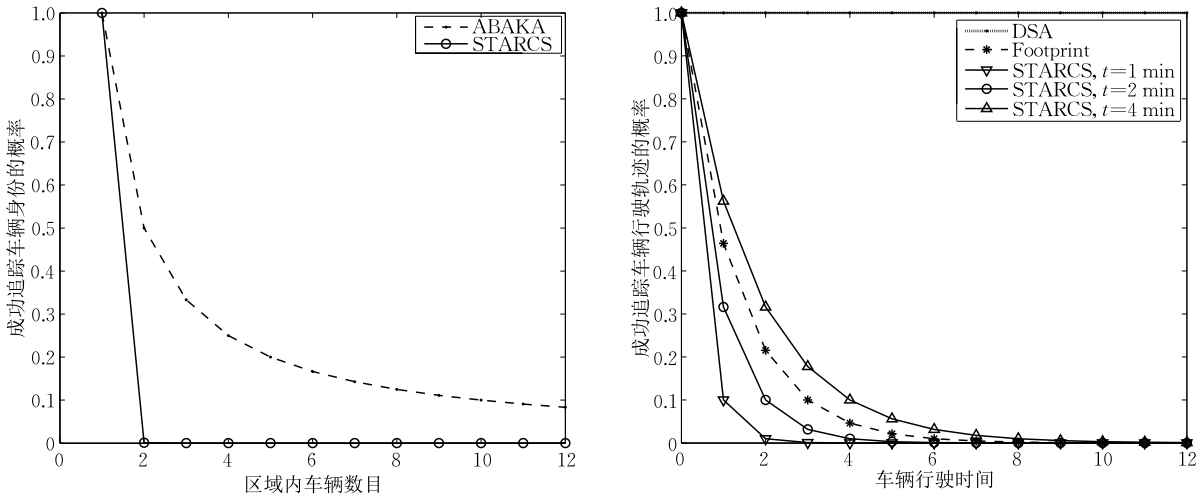
$$\begin{aligned} e(\sigma_{R_j}, P) &= e(sk^1_{R_j} + h(M')sk^2_{R_j}, P) \\ &= e(s_1 \cdot PID^1_{R_j} + h(M')s_1 H(PID^1_{R_j} \| PID^2_{R_j}), P) \\ &= e(PID^1_{R_j} + h(M')H(PID^1_{R_j} \| PID^2_{R_j}), PK_1). \end{aligned}$$

方案中时间戳标识是车辆在 VANETs 中唯一性身份，若合谋车辆将其正在使用的身份标识发送给攻击者使用，车辆通过比较同一警报事件的多个信息中是否存在相同的时间戳标识来检测出合谋 Sybil 攻击. 另外，若合谋车辆将自己不使用的身份发送给攻击者使用，本文根据时间戳标识中嵌入的 RSU 位置关系标签 L_{R_j}，检测出发送车辆位置出现不合理位移的情形，说明攻击者利用远距离的合谋车辆的身份发送虚假警报信息，检测出攻击者和远距离合谋车辆发动合谋 Sybil 攻击.

(4)匿名性和不可追溯性. 本方案采用了动态假名机制，车辆假名的使用以及动态更换保证了车辆在与 RSU 实现相互认证的过程中的匿名性. 车辆假名在进入不同 RSU 的通信范围内会生成不同的假名和签名，保证了同一车辆的不同消息之间的不可链接性，从而实现车辆的不可追溯性.

在无法获知车辆的真实身份时，若仅依靠对假名信息的收集来推测车辆的真实身份是很困难的. 下面建立一个概率模型来对攻击者能够成功追溯到某个车辆的真实身份的概率进行分析. 这个模型主要分析某个区域内车辆真实身份被捕获的概率和该区域范围内车辆数目的关系. 如图 6(a)所示，假设某区域内车辆数目为 n，在文献[18]的方案中用的是静态假名，假名不会变化，攻击者从 n 个匿名中成功区分出一个车辆的概率是 $P_A(n)=1/n$. 在本方案中，攻击者能够成功追踪到车辆真实身份的概率为 $P_S(n)=1/n^k$，其中，k 是车辆在区域内经过的 RSU 个数. 如果一个车辆经过了 10 个 RSU，则 $k=10$. 从图 6(a)中可以看出本方案中车辆身份被捕获的概率要远低于方案 ABAKA.

在 STARCS 中，RSU 同样采用了动态假名机制，RSU 在每个时间片内动态地改变假名防止攻击者根据 RSU 的位置推断出车辆的行驶轨迹. 如图 6



(a) 攻击者追踪到车辆真实身份的概率　　(b) 攻击者追踪到车辆行驶轨迹的概率

图 6　攻击者追踪到车辆真实信息的概率

(b)所示，假设某区域内 RSU 数目为 10，车辆每 3 min 经过一个 RSU. 由于 DSA[12] 中 RSU 对时间戳的签名中包含了 RSU 的具体位置，攻击者根据 RSU 的具体位置直接推断出车辆的行驶轨迹. Footprint[13] 中利用环签名对 RSU 发布的时间戳签名，则攻击者成功追踪到车辆行驶轨迹的概率为 $P_F(m)=1/m^{t/3}$，其中，t 为车辆行驶时间. 本方案中 RSU 利用了动态假名的方法，则攻击者能够成功追踪到车辆行驶轨迹的概率为 $P_S(n)=1/m^{t/\Delta t}$，Δt 是系统分割的时间片长度. 从图 6(b)中可以看出系统中时间片长短的变化会影响车辆被成功追溯到的概率.

(5) 条件隐私保护. 本方案采用了动态假名机制，一方面通过假名隐藏车辆的真实身份，另一方面仅允许可信权威机构 TA 根据车辆的假名追踪车辆的真实身份. 例如，车辆 V_i 发现车辆 V_j 以假名 PID_j 发送虚假的信息，车辆 V_i 会把车辆 V_j 的假名及签名消息汇报给可信机构 TA. TA 利用假名信息 PID_j 以及公钥 PK_j 根据式(7)追踪到车辆 V_j 的真实身份 RID_j，在保证车辆的真实身份不被泄露的情况下追踪恶意车辆，实现条件隐私保护的目的. TA 追踪到恶意车辆的真实身份之后，会根据撤销机制撤销该车辆. 同样，本方案利用动态假名机制来隐藏 RSU 的位置信息，车辆无法根据 RSU 的假名获知 RSU 的具体位置，更不会通过 RSU 的位置来追踪车辆的位置和行驶轨迹，但允许可信机构 TA 在验证车辆的请求信息时，根据 RSU 的假名获得 RSU 的具体位置，实现车辆位置信息的条件隐私保护.

6　性能分析与仿真

6.1　计算开销

本节主要通过验证时间戳标识的合法性和警报消息的签名来评价 STARCS 的计算开销. 假设道路上存在较多车辆，车辆需要对与其通信的多个车辆进行 Sybil 攻击检测. 为此，本文采用了批认证方法[19] 验证时间戳标识，并利用 ECDSA 算法对警报消息进行签名. 通过对比方案 Footprint[14] 和 SPASD[16] 分析本方法的计算开销. 其中，Footprint[14] 采用环签名方法[20] 发布签名形成身份轨迹，利用 ECDSA 算法对警报消息签名；SPASD 采用证书认证方法 ECMV[21] 发布标识并对警报消息签名. 表 4 为各种方案验证开销对比.

表 4　验证开销

方案	验证单条消息		验证 n 条消息	
	验证签名	验证身份	验证签名	验证身份
Footprint[14]	$4T_{mul}$	$27T_{exp}$	$4nT_{mul}$	$27nT_{exp}$
SPASD[16]	$3T_{par}+T_{mul}$	$3T_{par}+T_{mul}$	$3nT_{par}+nT_{mul}$	$3nT_{par}+nT_{mul}$
STARCS	$4T_{mul}$	$2T_{par}+T_{mul}+T_{mtp}$	$4nT_{mul}$	$2T_{par}+nT_{mul}+nT_{mtp}$

假设 T_{par} 表示执行一次双线性配对操作需要的时间，T_{mul} 表示执行一次乘法操作所需要的时间，T_{exp} 表示执行一次指数幂运算所需要的时间. 根据文献[22]可知，$T_{par}=3.21\,ms$，$T_{mul}=0.39\,ms$，$T_{mtp}=0.09\,ms$. 通过上述数据可知，执行一次双线性配对所需的时间和执行一次幂运算所需的时间基本相同. 对于其它一些运算，如单向哈希函数，这些运算所需要的时间集合可以忽略不计，所以在分析几种方法的计算性能时只考虑 T_{par}，T_{mul}，T_{exp} 和 T_{mtp} 这 4 个参数.

由于方案 Footprint[14] 利用车辆获得的多个 RSU 标识形成的轨迹作为身份信息，为此，需要对各个方案验证单条信息和批验证 n 条消息的计算开销进行比较. 从图 7 可以看出，无论是验证单条信息还是批验证多条信息，本方法所需的计算开销最短. 其中，SPASD 方案采用的 ECMV 只能对信息进行逐条验证，因此验证效率较低. Footprint 方案采用的环签名方法相比较普通签名方案的计算复杂度要高.

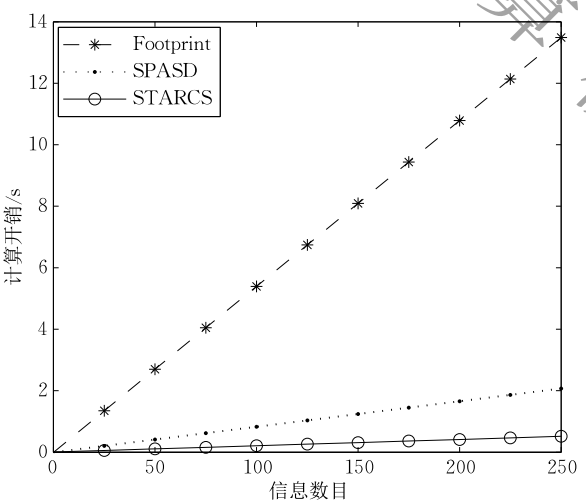


图 7 不同交通密度下的验证开销

6.2 通信开销

本文通信开销主要考虑签名以及信息中携带的假名以及证书，而车辆传递信息的内容本身并不将其考虑在内. 由于 Footprint[14] 随着轨迹的增加其通信开销也会增加，所以排除了方案 Footprint[14]. 对于方案[16]，签名长度是 42 字节，RSU 的标记是 44 字节，另外附带 121 字节的证书. STARCS 的通信开销包括签名长度为 42 字节，车辆临时假名为 42 字节，RSU_j 的假名为 44 字节，RSU 发布的时间戳标识为 21 个字节，消息时间戳为 4 字节. 表 5 为各种方案通信开销的对比，分别建立在认证单条信息和认证 n 条信息这两种情况下.

表 5 通信开销

方案	单条消息	n 条消息
SPASD[16]	207 bytes	$207n$ bytes
STARCS	153 bytes	$153n$ bytes

6.3 仿真实验

为了在较为真实的 VANETs 环境中测试 STARCS 方法的性能，本文使用 VanetMobisim 模拟车辆的动态轨迹，利用 NS-2 仿真从平均通信延迟和丢包率两个方面对 STARCS 方法和文献[14,16]进行对比. 主要的仿真参数如表 6 所示.

表 6 仿真参数

仿真参数	参数值
仿真时间	100 s
仿真场景范围	2000 m×2000 m
道路数量	Random
车辆数目	1～100 辆
车辆速度	10～30 m/s
移动录制时间步长	0.05 s
MAC 协议	802.11p
路由协议	AODV
发包频率	1 次/s

(1) 通信延迟

本节主要分析 V2V 之间的平均通信延迟，其结果与消息签名时间，消息验证时间以及消息包的大小有关. 平均通信延迟可定义为以下公式：

$$AD=\frac{1}{n}\sum_{i=1}^{n}(T_{sig}(i)+T_{trans}(i)+T_{ver}(i)) \quad (17)$$

其中，AD 表示平均通信延迟，n 表示发送车辆的数目，$T_{sig}(i)$ 表示车辆 V_i 签署消息的时间，$T_{trans}(i)$ 表示车辆 V_i 发送消息的传输时间，$T_{ver}(i)$ 表示接收车辆验证消息的时间.

一般情况下，随着车辆数目的增加，接收车辆的通信延迟越大. 如图 8 所示，当车辆密度不断增加时，本方案的通信延迟变化最小.

(2) 丢包率

丢包率是指在传输过程中消息丢包的概率，其形式化公式可定义为式(18). 其中，NrP 表示车辆接收到消息的包分组数目，NsP 表示车辆发送消息包的分组数目.

$$ALR=\frac{Nrp}{Nsp} \quad (18)$$

图 9 是STARCS 方法与Footprint[14] 和SPASD[16] 的消息丢包率对比图，从图中可以看出，STARCS 比这两种方法具有较小的丢包率. 当车辆密度较小时，由于车辆之间相距较远，丢包率较高，随着车辆密度

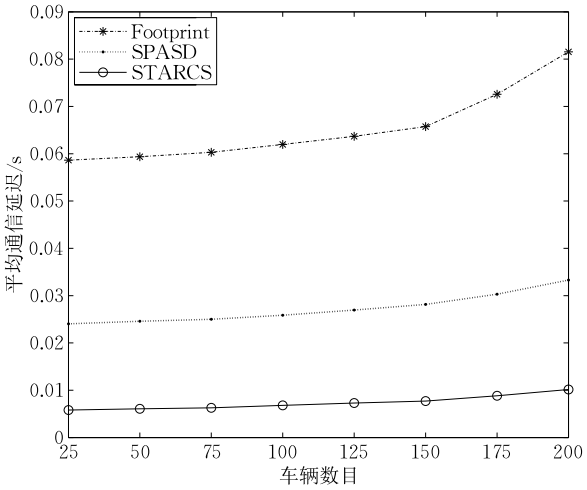


图 8　不同车辆密度下的平均通信延迟

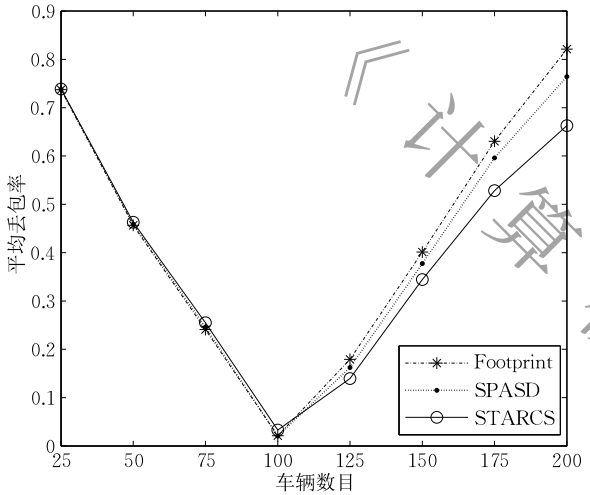


图 9　不同车辆密度下的丢包率

的增加丢包率会减小，但当车辆数目超过 100 时，丢包率会逐渐增加，这是因为多个车辆同时发送消息会产生数据碰撞导致数据包丢失.

(3) 漏报率和误报率

为了探究 STARCS 方法对攻击者与其它车辆合谋的检测效果，假设车辆在一分钟内都在同一个 RSU 的通信范围内，系统中有 10% 的合谋车辆. 由于车辆在行驶过程中，随着时间的增加，其获得 RSU 的时间戳标识逐渐增多，攻击者获得合谋车辆的时间戳标识的概率将会增加，因此需要对时间戳标识的有效使用时间进行设定. 本文为 RSU 发布的时间戳标识的有效时间设置了多种情况，图 10 为不同有效时间下检测到合谋 Sybil 攻击的对比图.

由图 10 可知，时间戳标识的有效时间越长，合谋车辆将会获得越多的身份信息，攻击者获得合谋 Sybil 身份的概率越高，从而导致漏报率随着有效时

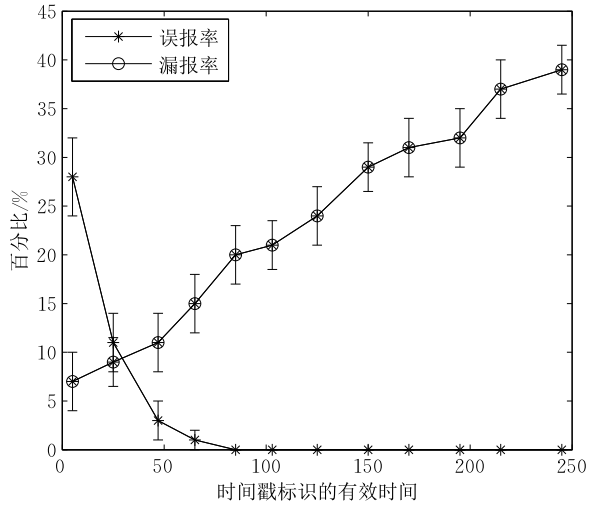


图 10　不同有效时间对误报率和漏报率的影响

间的增加而增加，但误报率在 1 min 的时候达到可接受水平.

另外，RSU 在整个系统中的部署情况及 RSU 的覆盖范围也会对合谋 Sybil 攻击检测具有较大的影响. 本文通过设定不同的 RSU 之间的最小距离，得到不同的部署方案对漏报率的影响，并设定 RSU 发布的时间戳标识的有效时间为 1 min. 图 11 为 RSU 部署间距对误报率和漏报率的影响.

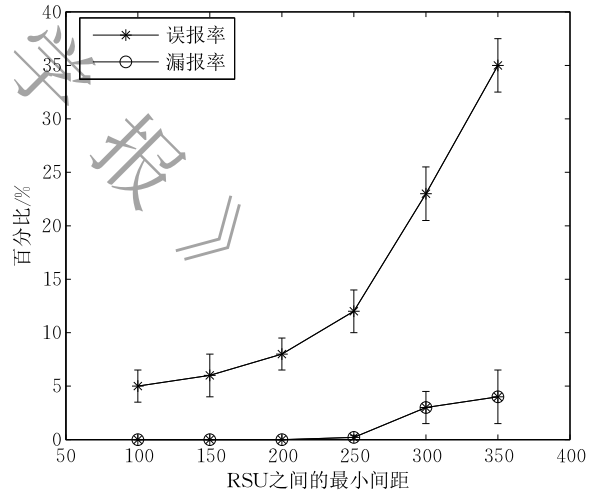


图 11　RSU 部署间距对误报率和漏报率的影响

由图 11 可知，当 RSU 的部署过于分散时，车辆的行驶轨迹过于模糊，车辆从 RSU 获得的时间戳标识的有效范围将大幅度提高，则合谋车辆将其身份提供给攻击者使用被检测出来的概率将会降低，漏报率会随之提高. 从图中可知，当 RSU 之间的间距达到 250 m 时，漏报率趋于稳定，当距离逐渐增加后，漏报率稍微增加，但误报率明显的提高，说明 RSU 间距越大，方案检测合谋 Sybil 攻击的性能越差.

7 总 结

本文对车联网中的 Sybil 攻击进行研究，主要为了抵制合谋 Sybil 攻击，并且平衡地解决 Sybil 检测和隐私保护这两个相互矛盾的问题，提出了一种基于时空分析的抗合谋 Sybil 攻击检测方法. 该方法利用匿名的 RSU 发布的时间戳标识作为 VANETs 中的车辆身份，车辆每进入新的 RSU 的通信范围，就会主动向 RSU 发送请求信息获取时间戳标识. 车辆发送警报事件信息时需要消耗 RSU 发布的时间戳标识，根据每个警报事件使用时间戳标识只能发送一次警报事件信息，通过检测时间戳标识是否被同一事件的多个信息使用检测 Sybil 攻击. 通过 TA 设置的请求信息表抵御伪造 Sybil 身份和合谋 Sybil 身份的产生. 依据标识中嵌入的基于 RSU 邻居关系的标签来检测出现不合理位移的合谋 Sybil 攻击. 为了防止检测 Sybil 攻击时泄露车辆的身份和轨迹信息，车辆和 RSU 均采用了动态匿名机制实现车辆的身份隐私和车辆运行轨迹隐私保护.

参 考 文 献

[1] Kaur N, Arora A. A research on various attacks in VANET. International Journal of Advanced Research in Computer Science, 2015, 6(6): 85

[2] Ghaleb F A, Zainal A, Rassam M A. Data verification and misbehavior detection in vehicular ad-hoc networks. Jurnal Teknologi, 2015, 73(2):37-44

[3] Feng X, Li C Y, Chen D X, et al. EBRS: Event based reputation system for defensing multi-source Sybil attacks in VANET//Xu K, Zhu H eds. Wireless Algorithms, Systems, and Applications. Cham, Germany: Springer International Publishing, 2015: 9204: 145-154

[4] Douceur J R. The Sybil attack//Proceedings of the 1st International Workshop on Peer-to-Peer Systems. Berlin, Germany: Springer, 2002: 251-260

[5] Saggi M K, Kaur R. Isolation of Sybil attack in VANET using neighboring information//Proceedings of the IEEE International Advance Computing Conference (IACC). Banglore, India, 2015: 46-51

[6] Kaur R, Malhotra N C J. Sybil attacks detection in vehicular ad hoc networks. International Journal of Advanced Research, 2015, 3(6): 1085-1096

[7] Feng X, Li C Y, Chen D X, et al. A method for defensing against multi-source Sybil attacks in VANET. Peer-to-Peer Networking and Applications, 2016, 10(2): 305-314

[8] Newsome J, Shi E, Song D, et al. The Sybil attack in sensor networks: Analysis & defenses//Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks. New York, USA, 2004: 259-268

[9] Zhou T, Choudhury R R, Ning P, et al. P2DAP-Sybil attacks detection in vehicular ad hoc networks. IEEE Journal on Selected Areas in Communications, 2011, 29(3): 582-594

[10] Yu B, Xu C Z, Xiao B. Detecting Sybil attacks in VANETs. Journal of Parallel and Distributed Computing, 2013, 73(6): 746-756

[11] Jin D, Song J S. A traffic flow theory aided physical measurement-based Sybil nodes detection mechanism in vehicular ad-hoc networks//Proceedings of the IEEE international Computer and Information Science (ICIS). Taiyuan, China, 2014: 281-286

[12] Park S, Aslam B, Turgut D, et al. Defense against Sybil attack in vehicular ad hoc network based on roadside unit support//Proceedings of the IEEE Military Communications Conference. Boston, USA, 2009: 1-7

[13] 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. Security and Communication Networks, 2013, 6(4): 523-538

[14] Chang S, Qi Y, Zhu H Z, et al. Footprint: Detecting Sybil attacks in urban vehicular networks. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(6): 1103-1114

[15] Hussain R, Oh H, Kim S. AntiSybil: Standing against Sybil attacks in privacy-preserved VANET//Proceedings of the IEEE International Conference on Connected Vehicles and Expo (ICCVE). Beijing, China, 2012: 108-113

[16] Hussain R, Oh H. On secure and privacy-aware Sybil attack detection in vehicular communications. Wireless Personal Communications, 2014, 77(4): 2649-2673

[17] Yang J H, Chang C C. An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Computers and Security, 2009, 28(3/4): 138-143

[18] Huang J L, Yeh L Y, Chien H Y. ABAKA: An anonymous batch authenticated and key agreement scheme for value added services in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 2011, 60(1): 248-262

[19] Liu Y, Wang L, Chen H. Message authentication using proxy vehicles in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 2015, 64(8): 3697-3710

[20] Tsang P P, Wei V K, Chan T K, et al. Separable linkable threshold ring signatures//Canteaut A, Viswanathan K eds. Progress in Cryptology-INDOCRYPT 2004. Berlin, Germany: Springer, 2004, 3348: 384-398

[21] Wasef A, Jiang Y, Shen X S. ECMV: Efficient certificate management scheme for vehicular networks//Proceedings of the IEEE Global Telecommunications Conference. New Orleans, USA, 2008: 639-643

[22] Horng S J T, Zeng S F, Pan Y, et al. b-SPECS+: Batch verification for secure pseudonymous authentication in VANET. IEEE Transactions on Information Forensics and Security, 2013, 8(11): 1860-1875

SHI Ya-Li, born in 1992, M. S. candidate. Her research interest is security of Vehicle Ad Hoc Networks (VANETs).

WANG Liang-Min, born in 1977, Ph. D., professor, Ph. D. supervisor. His research interests include information processing technology and security protocol of Internet of Things (IOT), security structure of Vehicle Ad Hoc Networks (VANETs).

Background

Vehicular Ad Hoc Networks (VANETs) is a special case of Mobile Ad Hoc Network (MANET) that has potential to enhance traffic safety and minimize congestion, thereby increasing driving efficiency, even provide value-added services application. In VANETs, vehicles communicate with each other, as well as with RSUs, through an open wireless channel, so VANETs is vulnerable to various attacks. Sybil attack is particularly easy to launch in VANETs due to its open and broadcast nature, which a malicious node poses as multiple other vehicles in order to gain disproportionate influence.

In Sybil attack, an attacker can forge its identity to masquerade as multiple other nodes, and obtain identity by stealing or by conspired with other vehicles. For example, a greedy driver create an illusion traffic congestion by transmitting fake messages using these identities at the same time, the rear vehicle receiving information will choose an alternate route to drive. Since Sybil attackers can control multiple identities, the attacker may destroy network protocols, such as routing protocols, resource allocation and malicious behavior detection mechanism, etc. In addition, Sybil attackers also with the help of multiple identities to launch other types of attacks, such as Denial of Service (DOS) attacks, black hole attacks, the wormhole attacks and so on.

However, the current schemes most only consider attacker launch Sybil attack on its own, such as attacker pretend to multiple identities by forging or stealing way. There are rarely detected program to consider attack conspired with other vehicles (we only consider conspired vehicles provide their identities to attacker actively). Due to attacker use legal identities of conspired vehicles, the existing detection scheme is difficult to detect conspiracy Sybil attack. In this paper, we proposed a kind resist conspiracy Sybil attack based on spatio-temporal analysis (STARCS). The method uses anonymous RSU released timestamp token as the identity in VANET and set the request information table by TA to record each vehicle last passed RSU and timestamp to resist forges and conspired Sybil identities generation. We check whether existing multiple alert messages of the same alert event have the same timestamp token to detect the Sybil attack, and based on the adjacent relation tag of RSU which embedded in the timestamp token to detect conspiracy Sybil attack.

This research is supported by the National Natural Science Foundation of China under Grant No. 61472001, the Major Research and Development Project of Jiangsu Province under Grant No. BE2015136.