# 车联网无线传感器网络 Sybil 攻击特点与检测方法研究

◆方晓汾[1]　郑丽辉[1]　厉国华[2]　方坤礼[1]　徐浩然[3]

（1.衢州职业技术学院机电工程学院　浙江　324000；2.衢州海西电子科技有限公司　浙江　324000；3.浙江金浙工业设备安装有限公司　浙江　324000）

摘要：智能汽车构成的智能交通系统中，复杂交通网络中的多类型传感器的能耗数据与传输的数据量日趋增加，由车载多源无线传感器构成的网络常遭到 Sybil 攻击，遭到攻击后将导致数据丢失甚至交通故障。Sybil 攻击以伪装身份或盗用正常节点的形式出现，但在车辆内部、车辆与车辆之间、车辆与基站之间通常所受到的攻击威胁侧重不同。本文分析了车联网中无线传感器网络拓扑结构及通信模式、受到 Sybil 攻击的特点、各检测方式，提出初期检测和能耗信任值计算的方式用于 Sybil 攻击网络节点的检测。

关键词：无线传感器网络；Sybil 攻击；车联网

基金项目：1.衢州市指导性科技攻关项目：智能驾驶的无线传感器网络攻击检测关键技术研究（No.2021069）；2.高校国内访问工程师校企合作项目：基于大数据的纯电动汽车驱系统状态监测关键技术研究（FG2019163）

无线传感器网络（Wireless Sensor Networks， WSN）是基于无线通信技术，由大量传感器节点以静止或移动、自组织的方式组网，集数据的采集、传输以及融合分析于一体的网络体系，在智能制造、智能楼宇、智能交通、环境监测、大数据健康等领域具有广泛的应用。无线传感器网络通过“末梢”——传感器节点采集电磁、温度、湿度、振动、图像、音频、视频等多种信息数据，且在网络中对多种信息数据进行综合处理。在整个无线传感器网络中，不具备防篡改的传感器节点处于开放式环境中，有部分甚至处于偏僻恶劣环境中，且其在网络中动态变化，导致了 Sinkhole、虫洞、Sybil 等一系列无线传感器网络攻击问题。

无线传感器网络安全包括主动攻击、被动攻击，主动攻击是通过未经授权的通信信道进行监听，从而篡改通信信道中的数据流信息；被动攻击则是通过隐藏的“节点”通过通信线路收集敏感数据[1]。无线传感器中存在消息认证、入侵监测以及访问权限等诸多网络安全。针对无线网络计算能力、节点能耗和通信能力等局限性进行恶意攻击，导致整个无线传感器网络异常，甚至瘫痪。Sybil 攻击由 John R. Douceur 于 2002 年首次提出[1]，是在对等网络（Peer to Peer）少数节点伪装成多个虚假身份，利用这些虚假的身份控制或影响网络正常网络节点，是目前无线传感器网络最为棘手的网络安全问题之一。

目前国内外针对无线传感器网络的 Sybil 攻击提出的监测方法较多，田英华等人[2]针对设备发射信号的信号频偏计算每台设备发射信号的频偏分布特征，识别伪造无线设备。薄尊旭等人[3]在区块链 P2P 的网络构架中 Sybil 攻击导致正常节点被篡改后进行识别，消耗正常节点计算资源，提出改进的 PBFT 共识算法中加入了 Pre-Commit 阶段来减少节点间通信的次数。徐宏等人[4-5]采用能耗检测的方式，利用马尔科夫模型为节点建立能耗预测模型。随着无线传感器在车联网（Vehicular Ad hoc Networks，VANET）的广泛应用，由于车辆本身处于行驶移动状态，车联网内的无线传感器构成的网络拓扑结构呈现出动态变化。陶敏等人[6]提出 VDP-SAD 算法依据 Beacon 消息为每辆车构建行驶模型矩阵（Driving Pattern Matrix， DPM），计算 DPM 的特征值评估车辆行驶模型的相似性，用于检测 Sybil 攻击节点。为了考虑到无线传感器网络计算时间开销、通信开销、通信延迟和丢包率，张春花等人[7]提出给每个车辆仅分配一个在特定区域内有效的短期标识（称为媒介访问码，Medium Access Code，MAC）的 Sybil 攻击抵御方法 SISD（Short-term Identification based Sybil attack Defense），胡倩儒[8]提出在车辆经过路边基础设施单元（Road Side Unit，RSU）时，向 RSU 申请时间戳，形成一条时戳链，当车辆分享路况信息时，必须附带自己的时戳链，其余车辆根据时戳链检测该车辆的历史轨迹与其他车辆的相似度，从而识别 Sybil 节点。在未来智能交通系统中，网络安全将是最为重要的部分，Hussain R 等[9-10]从智能交通系统 ITS 中车载自组织网络（VANet）的加密和非加密方法，用于处理和解决系统安全和隐私问题。冯睿琪等人[11]基于软件防护扩展（SGX）技术的车联网路况监测安全数据处理框架（SDPF），王新华等人[12] 阐述了电子认证技术、V2X 车联网公钥基础设施和各种 V2X 证书在车联网中的应用。由于车辆一直保持运动状态，两辆车在完全相同的时间点通过一系列路边基础设施单元 RSU 的情况几乎不可能，Park S[13]采用 RSU 产生时间戳序列方法和临时证书方法来判断任意两/多辆车在完全相同的时间点通过 RSU，从而识别是否遭受 Sybil 攻击。

综上所述，由于随着未来车辆进一步智能化，以及智能驾驶发展，车辆不再仅仅包括压力传感器、位置传感器、温度传感器、加速度传感器、角速度传感器，同时装备了用于环境感知的激光雷达、毫米波雷达、超声波雷达等智能传感器，车辆内部传感器无线自组织的方式形成多个节点传感器网络，车辆与车辆、车辆与路边基础设施单元之间同时也形成了多节点、多维度的无线传感器网络。由于无线传感器网络本身容易受到网络攻击和篡改，降低整个由智能汽车构成的智能驾驶交通网络的稳定性和安全性，实时持续监控网络内节点的行为和性能来评估节点的信任值来提高网络的安全性不仅计算量大，而且消耗过多的网络能耗资源，本文通过分析车联网无线传感器网络受到 Sybil 攻击的特点，在智能驾驶交通网络中，针对无线传感器网络提出对应的攻击检测方法。

## 1　网络拓扑与假设

### 1.1 网络拓扑

根据智能车辆装备的传感器构成的网络特点，分为由车辆内部、外部车辆共同构成、与外部交通系统无线传感器构成网络三个层面。

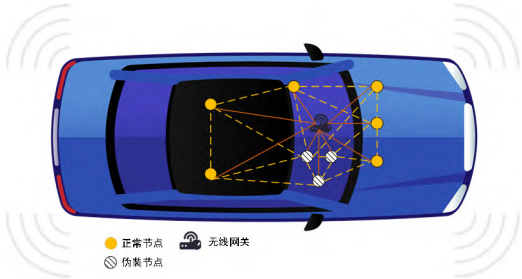


图 1 车辆内部无线传感器分簇式拓扑结构

车辆内部无线传感器以无线网关为中心，形成分簇式拓扑结构，如图 1 所示。无线传感器网络中节点位置固定，同一级传感器可进行相互通信。由于目前车辆内部的网络均采用总线式，其各种传感器采集的数据均需通过网关，而未来的智能汽车内部越来越多地采用无线传感器进行（P2P，Peer to Peer）自组网。

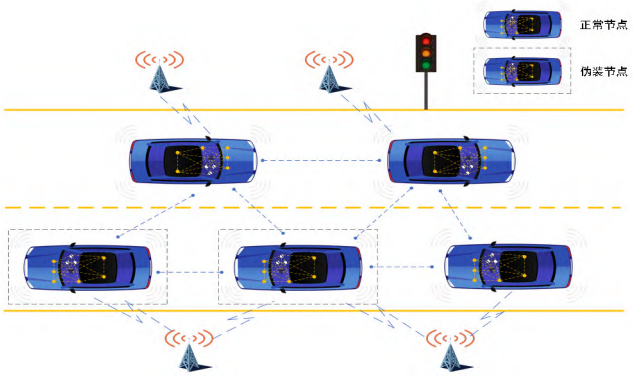


图 2 交通系统中车辆作为网络节点的拓扑图

智能车辆在道路运行过程中，由车辆与车辆、车辆与路边基础设施单元 RSU 之间形成的无线通信网络，如图 2 所示。其中，路边基础设施单元 RSU 包括基站，智能车辆无线网关作为网络节点在道路上，不断地重新自组网，并且与路边基础设施单元 RSU 不断地断网、自组网。其无线传感器组成的网络拓扑结构是随时间动态变化的，网络节点与节点之间是具有双向数据交换。

1.2 双向通信模型

无线传感器网络中网络节点互相之间存在数据的双向相互通信，Sybil 攻击情况下，车联网中部分智能汽车的节点会接收到多个位置信息，那么车联网会将受攻击后的错误位置和错误节点数目带入到具体算法中。

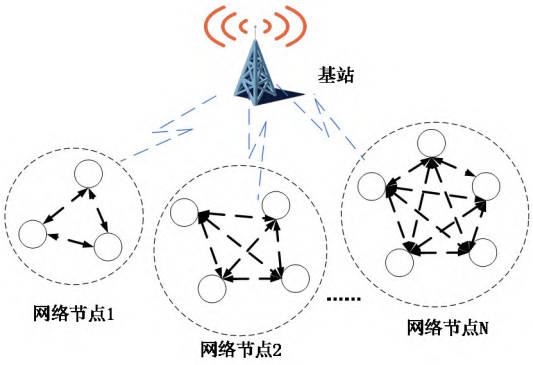


图 3 无线传感器网络双向通信模型

由于智能车辆内部存在无线传感器的局域网，由智能无线网关连接。当车辆行驶过程中，整个局域网是移动的，并且能够与基站进行双向的数据通信，如图 3 所示。

1.3 相关假设

假设 1：网络内有 N 个异构传感器节点，网络由基站节点、网络节点和传感器节点组成。

假设 2：基站不被攻击者破坏是可信的，并且基站资源不受限。

假设 3：网络内每个节点都具有唯一的 ID 和节点实时位置，车辆节点为移动的，智能传感器节点相对车辆节点为固定位置。

## 2 车联网 Sybil 攻击特点

网络内的传感器节点在指定的频率将采集的数据连同信息表 1 发送至对应的网络节点。

表 1 路由数据信息表

| ID | Position | Time | State |
|---|---|---|---|

表 1 中的 ID 为节点身份唯一标识，Position 为节点的静态位置，Time 为数据的采集时刻，State 为节点状态信息。传感器节点每次向网络节点发送路由数据时，将更新自身信息表中 Time、State 的值。网络节点在指定的频率将采集的数据连同信息表 1 发送至对应的基站节点。

2.1 身份 ID 与位置信息

身份 ID 与实体节点所在位置一一对应是网络正常运行的基础。在智能车辆内部，不同的无线传感器网络出现伪装节点，一旦某一传感器节点受到 Sybil 攻击，由于伪装节点通过发送错误的信息，导致无线传感器其他节点对正常节点的位置信息、状态信息等进行误判，导致整个系统出现严重的破坏。例如，智能冷却液温度传感器被 Sybil 攻击后，伪装的智能冷却液温度传感器节点将向网络中传输错误的信息，从而导致整个网络系统基于错误的信息作出判断。

智能车辆传感器节点仅在车辆内部采集数据，由智能网关构成传感器无线网络，其节点数有限，网络拓扑结构固定，采集范围有限，通信范围可控等。伪造新身份的 ID 往往较为容易进行识别和判断，所以 Sybil 攻击通常表现在盗用正常节点对网络进行破坏。

针对智能车辆在移动过程中，车辆相对临近车辆的位置以及由多个智能车辆构成无线网络再与基站进行通信，智能车辆相对基站是移动的。网络节点都处在变化状态，导致网络拓扑结构频繁地随时间变化而变化。Sybil 攻击通常表现为伪造新身份 ID 或盗用正常节点两种形式，由于智能车辆不断加入新的无线传感器网络中，需要基于位置获取新的身份 ID，那么在这个动态变化的过程中，Sybil 无论是伪造新身份 ID 还是盗用正常节点都是难以被识别和检测。导致整个智能交通网络误判以致系统瘫痪。

2.2 车联网通信特点

车联网（Internet of Vehicle，IoV）通过智能传感器采集车辆工作状态信息、环境信息，并通过车辆、行人、道路交通设施之间网络进行数据交互。车联网体系包括感知层、网络层、应用层，其中感知层处于最底层，包括物理层与数据链路层。智能车辆通过收集车辆行驶过程中的状态数据、交通信息、道路环境信息。其中通信交互包括车辆与车辆之间通信（Vehicle to Vehicle，V2V）、车辆与交通基础设施（Vehicle to Infrastructure，V2I）、车辆与行人通信（Vehicle to Pedestrian，V2P）。

车联网由于智能车辆为实时移动的，所以导致网络拓扑结构频繁变化，车辆在高速行驶时，车辆之间的链路连接仅维持 10 秒以内，且连接链路不稳定。车联网中智能车辆作为网络节点，其产生大量的数据量，数据在采集、处理、存储过程中的隐私安全直接关系到整个交通安全。针对车联网本身的特点，影响车联网数据安全最为直接的是未经授权即可访问这些数据，导致数据被非法访问，甚至恶意篡改。

2.3 Sybil 攻击方式

按照攻击节点如何获取非法身份并与真实节点进行通信方式，可以将 Sybil 攻击分为直接通信攻击和间接通信攻击。直接通信即 Sybil 节点与正常节点直接进行通信，恶意节点可通过 Sybil 节点对信息进行实时监听，且 Sybil 节点向正常节点发送恶意信息。间接通信是多个恶意节点在网络中声称可以通过其链路到达 Sybil 节点，正常节点与 Sybil 节点不直接通信。

从攻击如何获取身份 ID 的角度，Sybil 惯用的攻击方式即为伪造身份与偷窃身份，伪造身份即在网络中构造出多个任意的 Sybil 节点的身份 ID，从而使得网络中存在多个实际“不存在”的网络节点。偷窃身份即考虑到无线传感器网络中不能无条件地伪造出一些“不存在”的网络节点，“不存在”的网络节点也不能通过身份认证，那么 Sybil 攻击采用将正常节点进行破坏和失效，从而获得正常节点的身份 ID，从而使得正常节点转变为 Sybil 节点。例如，智能车辆内部传感器网络不能无条件多出众多“不存在”的传感器硬件设备，那么只能通过盗用身份的方式进行攻击。

根据 Sybil 节点多个身份 ID 的“不存在”节点是否同时参与网络通信，Sybil 攻击分为同时攻击和非同时攻击。同时攻击指的是 Sybil 节点利用所有身份 ID 同时参与网络通信。非同时攻击指的是 Sybil 节点多个身份 ID 在某一时刻仅用一个身份 ID 进行通信，其他身份 ID 退出网络通信。例如，多辆智能车辆行驶在道路上，其中，某一辆智能车辆与相邻智能车辆共同组成无线传感器网络簇，该车辆一攻击成为 Sybil 节点，就拥有多个身份 ID，采用同时攻击模式下，相邻智能车辆不能判断周围智能车辆的数量以及交通工况，且消耗网络资源，使得真实智能车辆节点难以加入该网络簇，影响交通正常通行。而如果在非同时攻击模式下，则相邻智能车辆会识别出不断有新的智能车辆加入该网络簇，如图 4 所示。

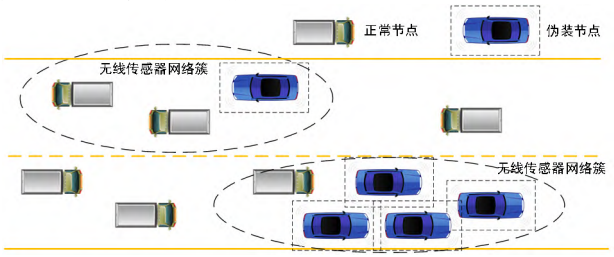


图 4 道路行驶智能车辆之间同时攻击与非同时攻击

## 3 检测方法

3.1 初期检测

为了检测无线传感器网络中节点身份 ID 不一致，以及在数据采集时刻 Time 下，静态位置信息 Position、节点状态 State 具有异常时，静态位置信息 Position 异常计算：

$$d_x = P_x - \bigcap_{i=1}^{j}(P_i, r_i)$$

式中，在某时刻 t，$P_x$ 为某一智能车辆节点所在的空间位置，$P_i$ 为网络簇中第 i 辆智能车辆所在空间位置，$r_i$ 为第 i 辆智能车辆有效通信半径，$d_x$ 为某一智能车辆距离网络簇中心的距离，超过阈值则判断该节点位置信息 Position 异常。

当智能车辆节点 ID 一致，但在 t 数据采集时刻，且同一路段静态位置信息 Position 范围内的网络簇中，某车辆状态数据 State（速度、冷却液温度、发动机转速等），与同一网络簇中相邻车辆相差值超过阈值，则判断该智能车辆节点已受到 Sybil 攻击，其产生的数据包将

被丢弃。

3.2 能耗信任值计算

能耗信任值是针对车联网中网络节点被 Sybil 攻击后伪造合法的节点身份 ID 和静态位置信息 Position，基于网络节点能耗信任值的计算即针对每一网络节点剩余能量 $E_{res}$ 与其初始能量 $E_0$ 关系，

$$E_0 \geq E_{res} + E_{avg} + \tau$$

$E_{avg}$ 当前网络节点所在网络簇内所有成员节点已经消耗的平均能量，τ 为能量补充值，根据所在工况进行调整。

基于智能车辆网络节点检测 Sybil 攻击的任务，其中具体的算法实现步骤如下所示：

| 智能车辆网络节点检测 Sybil 攻击： |
|---|
| Input：ID、Position、Time、State、$E_{res}$ 和网关融合的数据 |
| Output：识别网络中节点 Sybil 攻击 |
| Algorithm：<br>(1)基站接收智能车辆网络节点网关数据包；<br>(2)基站通过智能网关的 ID 和 Position 初期检测；<br>(3)If CH（ID， Position， Time， State） match R ， then<br>(4)If $E_0 \geq E_{res} + E_{avg} + \tau$，then<br>(5)S++；<br>(6)Else<br>(7)U++；<br>(8)If $T_{bs,x}(\Delta t) \geq 5$， then<br>(9)基站接收该网络节点网关数据包；<br>(10)Else<br>(11)转到步骤（13）；<br>(12)Else<br>(13)存在 Sybil 攻击，丢弃发送的数据包；<br>(14)End |

3.3 不同层级 Sybil 攻击检测比较

在车联网中，不同层次的无线传感器构成的网络其复杂度不同，拓扑结构不同，面临的 Sybil 攻击特点也不同，针对不同层次的 Sybil 攻击所采取的策略也不同。按照智能车辆内部、车辆、交通系统三个层次进行划分，如表 2 所示。

表 2 不同层级网络 Sybil 攻击检测比较

| 节点构成 | 攻击难易 | 检测难易 | 等级 |
|---|---|---|---|
| 由车辆内智能传感器构成，位置、数量固定，总线式通信 | 难 | 易 | S1 |
| 由智能车辆作为网络节点，位置、数量变化大，网状式 | 易 | 难 | S2 |
| 由基站与智能车辆构成的网络簇进行交互，一方移动，相对位置、数量不固定 | 易 | 难 | S3 |

由于智能车辆包含了 60~100 个传感器，车辆的 CPS 组件（传感器、设备、系统）之间存在着高度的耦合、内聚力。感知、通信和控制层多层交互作用，感知层或通信层中的网络攻击会危及控制层的安全性，特别是车辆动力学传感器（轮胎压力监测系统（TPMS）、磁编码器和惯性传感器）和环境传感器（例如光探测和测距（LiDAR）、超声波、照相机、无线电探测和测距系统（雷达）和全球定位系统（GPS））更为突出。在车联网系统中，所以针对由智能车辆作为网络节点构成的无线传感器网络进行快速有效的检测和攻击识别至关重要。

## 4 总结

本文提出了智能车辆构成的智能交通系统里，车辆由车联网连接通信，分析在无线传感器网络中 Sybil 攻击特点。Sybil 通常以伪装身份、盗用正常节点为主要攻击手段，多个节点同时或非同时发起攻击，包括有隐蔽性较好，难以进行检测的非直接攻击方式。融合初步检测和能耗信任值计算方法，针对不同层级 Sybil 攻击与检测进行了对比分析，智能车辆在智能交通系统中安全高效运行，交通数据的全生命周期安全将面临严峻挑战。在后续的工作中，将深入智能交通系统中其他威胁交通数据安全的攻击、漏洞检测。

## 参考文献：

[1]Douceur J R . The Sybil Attack[C]// Springer，Berlin，Heidelberg. Springer，Berlin，Heidelberg，2002.

[2]田英华，郑娜娥，张靖志，等.基于频偏分布的无线局域网 Sybil 攻击检测方法[J].信息工程大学学报，2020，21（03）：290-296.

[3]薄尊旭. 基于改进 PBFT 算法的区块链中 Sybil 攻击防御方法研究[D].北京工业大学，2020.

[4]徐宏，江波，谢金辉.WSNs 中基于节点能耗特征的入侵检测模型研究[J].电子设计工程，2022，30（03）：108-112.

[5]方晓汾，方凯，汪小东，等.基于能耗信任值的无线传感器网络 Sybil 攻击检测方法研究[J].传感技术学报，2020，33（06）：907-915.

[6]陶敏，关胜利，崔鹏飞.基于车辆行驶模型的 Sybil 攻击检测算法[J].实验室研究与探索，2021，40（11）：71-74+110.

[7]张春花，马竟宵.车联网中基于短期标识的 Sybil 攻击防御方法[J].小型微型计算机系统，2021，42（08）：1727-1734.

[8]胡倩儒. 车联网中 Sybil 攻击及虚假消息检测技术研究[D].西安理工大学，2021.

[9]Hussain R，J Lee，Zeadally S. Trust in VANET：A Survey of Current Solutions and Future Research Opportunities[J]. IEEE Transactions on Intelligent Transportation Systems，2020（99）：1-19.

[10]Lu Z，Qu G，Liu Z . A Survey on Recent Advances in Vehicular Network Security， Trust， and Privacy[J]. IEEE Transactions on Intelligent Transportation Systems，2018：1-17.

[11]冯睿琪，王雷蕾，林翔，等.基于 SGX 的车联网络况监测安全数据处理框架[J/OL].计算机应用：1-10[2022-07-05].

[12]王新华，李广超，王本海，等.电子认证在 V2X 车联网安全中的应用[J].信息安全研究，2022，8（05）：500-505.

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

# 高校无线网络泄密风险分析与应对策略

◆姜少杰　王绍朋　刘颖慧　刘学洪

（四川大学信息化建设与管理办公室　四川　610000）

摘要：防止敏感或涉密信息通过网络泄漏是网络安全以及涉密管理中至关重要的一部分，高校无线网络的开放性、便捷性对该项工作提出了更高的挑战。本文分析了高校在涉密管理中的无线安全问题，并结合高校网络的组网特点、人员构成以及不同接入环境，提出了泄密风险的综合评估办法，并从管理和技术上提出了可行的应对方案。

关键词：无线局域网；网络安全；涉密管理

基金：四川大学社科研究项目“高校无线网络泄密风险分析及应对策略”（项目编号：skbm202105）