

面向降频污染攻击的智能交通拥堵态势量化分析*

相迎宵^{1,2}, 李轶珂^{1,2}, 刘吉强^{1,2}, 王潇瑾^{1,2}, 陈彤^{1,2}, 童恩栋^{1,2}, 牛温佳^{1,2}, 韩臻^{1,2}



¹(智能交通数据安全与隐私保护技术北京市重点实验室, 北京 100044)

²(北京交通大学, 北京 100044)

通信作者: 童恩栋, E-mail: edong@bjtu.edu.cn; 牛温佳, E-mail: niuwj@bjtu.edu.cn

摘要: 随着网联车辆的快速发展和开放化, 智能信号灯规划系统承受着巨大的网络攻击风险. 已有相关研究发现, 定频数据污染对规划脆弱性的攻击造成了交通拥堵爆增, 但缺乏对降频污染攻击的全时序拥堵态势量化与分析, 在检测预警与持续对抗方面有一定的局限性. 将开源智能信号灯规划系统 I-SIG 及其规划算法 COP 作为研究对象, 提出一种面向多个降频污染攻击的统一拥堵态势量化与分析框架, 构造态势发展的时空序列三阶张量空间, 并设计极值分析、平稳性分析和关联性分析, 实现基于函数依赖关系的一体化分析方法. 在交通模拟环境 VISSIM 平台上, 验证了该量化分析的有效性并报告新发现.

关键词: 污染攻击; 拥堵态势; 量化分析; 智能交通; 张量空间

中图法分类号: TP309

中文引用格式: 相迎宵, 李轶珂, 刘吉强, 王潇瑾, 陈彤, 童恩栋, 牛温佳, 韩臻. 面向降频污染攻击的智能交通拥堵态势量化分析. 软件学报, 2023, 34(2): 833–848. <http://www.jos.org.cn/1000-9825/6416.htm>

英文引用格式: Xiang YX, Li YK, Liu JQ, Wang XJ, Chen T, Tong ED, Niu WJ, Han Z. Quantified Analysis of Congestion Situation in Intelligent Transportation Towards Frequency-reduced Spoofing Attack. Ruan Jian Xue Bao/Journal of Software, 2023, 34(2): 833–848 (in Chinese). <http://www.jos.org.cn/1000-9825/6416.htm>

Quantified Analysis of Congestion Situation in Intelligent Transportation Towards Frequency-reduced Spoofing Attack

XIANG Ying-Xiao^{1,2}, LI Yi-Ke^{1,2}, LIU Ji-Qiang^{1,2}, WANG Xiao-Jin^{1,2}, CHEN Tong^{1,2}, TONG En-Dong^{1,2}, NIU Wen-Jia^{1,2}, HAN Zhen^{1,2}

¹(Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing 100044, China)

²(Beijing Jiaotong University, Beijing 100044, China)

Abstract: With the development and openness of connected vehicle, the planning system of intelligent signal system (I-SIG system) has a big security threat from network attack. Former work has revealed that a frequency-fixed data spoofing attack to the planning weakness can cause a heavy traffic congestion. However, there is still very limited knowledge for security detection, warning, and defense, and there is no work that provides a full time-serial congestion situation quantification and analysis for various attack frequency from high to low. Targeting the open source I-SIG system and its COP planning algorithm, this study proposes a unified framework to quantify and analyze the congestion situation under multiple spoofing attack from high to low frequency. Firstly, a space-time tensor space of three orders is constructed. Based on tensor computation, a function-dependent integrated analysis approach is implemented, in which the max-min analysis, stationarity analysis, and correlation analysis are developed. Experiments on the traffic simulation platform VISSIM show the effectiveness of quantification and analysis, and demonstrate that the results are meaningful.

Key words: spoofing attack; congestion situation; quantified analysis; intelligent transportation; tensor space

* 基金项目: 中央高校基本科研业务费专项资金 (2021JBM006); 国家自然科学基金 (61972025, 61802389, 61672092, U1811264, 61966009); 国家重点研发计划 (2020YFB1005604, 2020YFB2103802)

收稿时间: 2020-12-21; 修改时间: 2021-05-08, 2021-06-15; 采用时间: 2021-06-28; jos 在线出版时间: 2022-07-15

CNKI 网络首发时间: 2022-11-16

随着人工智能 (artificial intelligence, AI) 等先进技术的引入, 智能交通系统 (intelligent transportation system, ITS)^[1]以实现安全有保障的高效综合运输系统为目标, 受到越来越多的政府部门、科研机构与科技企业的关注, 正在迈入基于 AI 的新一轮研究创新与工业落地实践双轨并行的阶段. 特别是一些子系统如基于车辆感知的单路口智能信号灯规划系统 (intelligent traffic signal system, I-SIG)^[2], 由于具有高性能和易部署的特点, 已经被广泛应用. 美国交通部 USDOT 于 2016 年已经开始试点在纽约市、佛罗里达州坦帕、怀俄明州夏延、亚利桑那州坦普尔和加利福尼亚州帕洛阿尔托等城市街道部署 I-SIG 智能交通信号灯规划系统, 实际可以降低 26.6% 的车辆通行延时. 中国交通部依托滴滴出行于 2018 年在山东省济南市的 344 个道路交叉口试点智能交通信号灯系统, 实际可以降低 10%–20% 的车辆通行延时. 同时, 地方政府也在积极投入并开展部署试点, 其中典型的有北京海淀区后厂村和上海浦西世博园等, 都取得了良好的效果. 可以预见, 未来 I-SIG 将具有非常大的实用和落地潜力, 成为解决交通安全性和提升交通运行效率不可或缺的智能系统.

I-SIG 主要涉及 3 类对象: 依赖终端接入的网联汽车 (connected vehicle, CV)^[3,4]、智能信号灯控制系统以及承载数据与控制指令的通信网络. 随着网联车辆的快速发展和开放化, I-SIG 承受着巨大的网络攻击风险. NDSS2018 的一篇工作^[5]发现了定频数据污染对规划脆弱性攻击造成了交通拥堵爆增, 一辆攻击车辆发起的轨迹数据污染攻击在短短 8 分钟就让堵塞达到了 236%. 后续相关工作^[6,7]对 I-SIG 的攻击开展了特征工程及面向预测的监督模型学习. 然而, 已有工作都是针对最高污染攻击频率, 即数据污染的间隔在 1 个规划阶段左右, 而不考虑其他低频率攻击. 实际上, 攻击者为提高攻击隐蔽性, 低频率攻击是存在的. 此外, 已有工作聚焦的是端到端的攻击效果分析, 并未在方法和实验上呈现过程性的全时序拥堵态势分析, 不利于检测预警与持续对抗能力的提升.

针对上述局限, 本文提出了一种面向多个降频污染攻击的统一拥堵态势量化与分析框架, 将智能信号灯规划系统 I-SIG 及其规划算法 COP^[8,9]作为研究对象, 通过构建时空序列的三阶张量空间, 在感知基础上设计基于张量的极值分析、基于自相关的平稳性分析、基于不同聚类簇的关联性分析, 并最终实现基于函数依赖关系的一体化分析方法. 本文的贡献点主要有 3 个方面.

(1) 提出面向多个降频污染攻击的统一拥堵态势量化框架, 通过正交攻击频率维、攻击相关空间特征维与时序维, 构建了时空序列的三阶张量空间, 提供不同频率的多维感知交叉视角; 该框架针对性地服务于智能信号灯规划系统 I-SIG 在持续攻击状态下的单路口拥堵态势感知;

(2) 基于函数依赖关系设计了 3 种分析相关联的一体化分析方法, 包括基于张量的极值分析、基于自相关的平稳性分析、基于不同聚类簇的关联性分析, 为后续自动化工程实现提供支持;

(3) 在交通模拟环境 VISSIM 平台上, 针对 8 信号灯相位的单路口, 实现了 5 种频率持续攻击下的 30 分钟交通流量实验, 发现了新的实验结果, 包括降频攻击仍然可产生明显的攻击效果、低频攻击下容积率和拥堵度具有更稳定的自相关系数表征.

1 预备知识

1.1 智能信号灯系统网络基础

I-SIG 系统的空-天-地一体化网络架构如图 1 所示, 主要包含两个部分: 空间部分和地面部分. I-SIG 系统的 CV 环境属于地面部分. CV 环境主要包含 3 个组件: 车载单元 (on-board units, OBUs)、路边单元 (road-side units, RSUs) 以及信号灯规划单元, 它们分别是安装在车辆、路边服务器以及交通信号灯上的设备. 车到车 (vehicle to vehicle, V2V)^[10]、车与基础设施 (vehicle to infrastructure, V2I, 如路边服务器)^[11]的通信采用的是专用短距离通信协议 (dedicated short range communications, DSRC)^[12], 是一种基于 802.11p 的无线通信, 提供信道并能实现高速直接通信. 每辆车以匿名的方式向周围车辆广播基本安全消息 (basic safety messages, BSM). 作为一种关键的信息载体, BSM 包含了车辆大小、位置、速度、行驶方向、加速度以及刹车系统状态等核心数据. 与 DSRC 相比, RSU 与信号规划单元的通信采用的是 NTCIP 协议 (national transportation communications for intelligent transportation system protocol)^[13]. 通过提供车辆和交通信号之间的双向通信, NTCIP 支持不同制造商的计算机和电子交通控制设备.

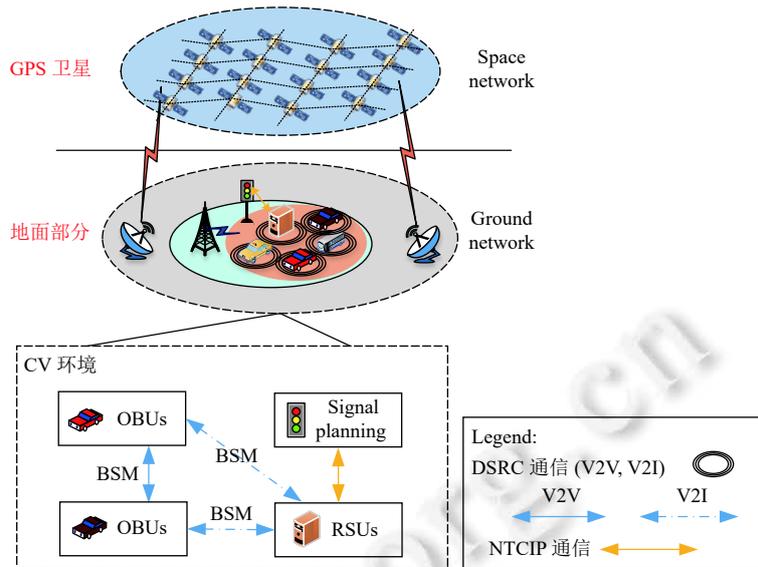


图 1 I-SIG 系统的空-天-地一体化网络架构

1.2 最后车辆数据污染攻击

I-SIG 系统的数据流如图 2 所示. 车辆上的 OBU 通过广播 BSM 消息发送车辆的实时轨迹数据; RSU 收集车辆轨迹数据, 并处理这些数据形成到达表 (如表 1); 到达表作为输入发送给包含 COP 算法和 EVLS 算法的信号规划单元. 如果 OBU 装配率 (penetration rate, PR) 小于 95%, EVLS 算法会被调用执行, 更新到达表中的数据. 否则, COP 算法直接根据到达表中的数据对信号灯时长和相位序列进行规划. 根据 COP 算法的结果, 信号规划单元向相位控制器发送信号灯控制指令. 在信号控制的每个阶段后, 信号灯状态作为反馈返回给信号规划单元.

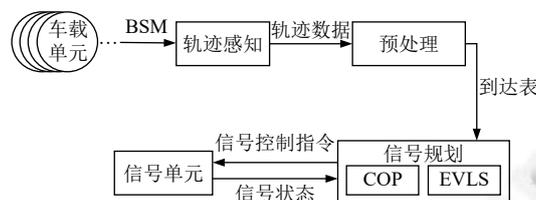


图 2 I-SIG 系统数据流

表 1 到达表

Arrival time (T_M)	Phase			
	1	2	...	8
T_0	N_{01}	N_{02}	...	N_{08}
T_1	N_{11}	N_{12}	...	N_{18}
T_2	N_{21}	N_{22}	...	N_{28}
...
T_M	N_{M1}	N_{M2}	...	N_{M8}

表 1 中, $T_i = i (0 \leq i \leq M)$ 代表车辆从当前位置达到停止杆 (设置在信号灯前停止线的位置) 的时间. I-SIG 系统中, $M=130$ s, 覆盖了超过两分钟的 BSM 消息统计. $N_{ij} (i \in [0, M], j \in [1, 8])$ 表示在相位 j , 有 N_{ij} 辆车将会在 T_i 秒内到达停止杆. 本文的交叉口信号灯场景中, I-SIG 系统设置 8 个信号灯, 分别对应 8 个相位, 包含 4 个直行相位

和 4 个左转相位.

如果联网车辆比例不够高 (装配率 < 95%), COP 算法的规划效果就会大大降低. 因此, I-SIG 利用联网车辆的轨迹数据, 用 EVLS 算法估计真实的排队长度, 基于 Wiedemann 的跟车模型来填充监控路段的空白部分, 并在联网车辆之间填充车辆数据. 排队队列开始于停止杆, 因此, 需要确定排队队列的最后车辆来确定队列长度. EVLS 算法估计排队车辆步骤如下: (1) 最后停止的联网车辆与倒数第二辆停止的联网车辆的停止时间和距停止杆的距离分别表示为 T_{q1}, L_{q1}, T_{q2} 和 L_{q2} 当前时间为 T_C , 估计排队长度表示为 L_{es} . 假设队列传播速度 v_q 是常数, 则 v_q 为: $v_q = (L_{q1} - L_{q2}) / (T_{q1} - T_{q2}) = (L_{es} - L_{q1}) / (T_C - T_{q1})$; (2) 估计的排队长度 L_{es} 为: $L_{es} = L_{q1} + v_q (T_C - T_{q1})$; (3) 若平均车辆长度为 C , 排队车辆数 N_{0i} 的计算公式为: $N_{0i} = \lceil L_{es} / C \rceil, i \in [1, 8]$.

两种最后车辆数据污染攻击的策略如图 3 所示, 第 1 种策略是不考虑装配率的情况下, 直接攻击到达表; 第 2 种策略是装配率小于 95% 时, 攻击 EVLS 以间接攻击到达表. 第 1 种策略属于到达时间和相位的数据欺骗攻击, 攻击者通过修改车辆的 BSM 消息中的速度和位置信息, 改变车辆的到达时间及其所请求的相位. 无论 PR 是多少, 这种攻击策略可以直接攻击输入数据流. 如图 3(a) 所示, 攻击者在原始车辆队列后的任意位置添加欺骗车辆, 作为一辆最晚到达车辆, 使得车辆队列变长, 导致 COP 算法分配给当前相位的绿灯时间增加, 进而延迟所有相位的下一次绿灯开始时间, 造成拥堵. 第二种策略是排队长度欺骗, 通过修改 BSM 消息中的位置和速度值来增加 EVLS 算法估计的排队长度. 如图 3(b) 所示, 攻击者添加一辆距离停止杆最远的车辆. 由于 EVLS 算法是根据最后一辆停止车辆的位置来估计排队长度的, 因此攻击可以造成估计的排队长度 L_{es} 增加, 以及排队车辆数 N_{0i} 的增加.

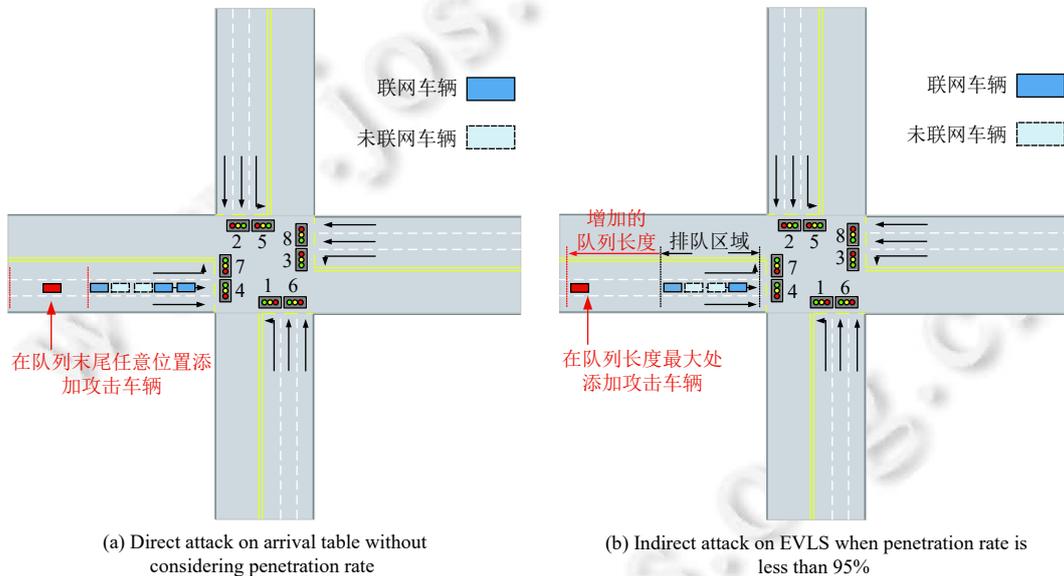


图 3 数据污染攻击的两种策略

2 拥堵态势量化分析

2.1 问题定义

定义 1 (容积率). 设每个相位的最大车容量为 C_k^{\max} , 所有 8 个相位的车容量 $C_{\text{total}}^{\max} = \sum_{k=1}^8 C_k^{\max}$, 则路口的车辆容积率为: $CR = (\sum_{k=1}^8 N_k) / C_{\text{total}}^{\max}$, 其中, N_k 是第 k 个相位上的车辆数.

定义 2 (拥堵度). 设 Q_k 为第 k 个相位的排队车辆数, Q_{normal} 是正常允许的排队车辆数, 则相位 k 的拥堵度为: $PCD_k = Q_k / Q_{\text{normal}}$. 路口的拥堵度为: $ICD = \sum_{k=1}^8 PCD_k$.

定义 3 (攻击加速度). 设 t_0 为攻击开始的时刻, 则 t 时刻的容积率攻击加速度、相位 k 拥堵度攻击加速度、

路口拥堵度攻击加速度分别为: $\alpha_{CR}(t)=(CR(t)-CR(t_0))/(t-t_0)$, $\alpha_{PCD}(t, k)=(PCD(t, k)-PCD(t_0, k))/(t-t_0)$, $\alpha_{ICD}(t)=(ICD(t)-ICD(t_0))/(t-t_0)$.

定义 4 (攻击放大比). 设 t_0 为攻击开始的时刻, 则 t 时刻的容积率攻击放大比、相位 k 拥堵度攻击放大比、路口拥堵度攻击放大比分别为: $\beta_{CR}(t)=CR(t)/CR(t_0)$, $\beta_{PCD}(t, k)=PCD(t, k)/PCD(t_0, k)$, $\beta_{ICD}(t)=ICD(t)/ICD(t_0)$.

问题定义 5 (变频攻击序列化分析). 给定最晚到达时间阈值 M , 平均车辆长度 C , 初始攻击时刻 t_0 , 对任意的攻击频率 $f \in \mathbf{f}=\{f_1, f_2, \dots, f_p\}$, 设观察时间间隔为 Δt , 则当前时刻为 $t=t_0+n\Delta t(n \in N_+)$, 对应的宏观态势向量和微观态势向量分别为 $\mathbf{s}_{macro}(t, f)=(CR(t), ICD(t), \alpha_{CR}(t), \alpha_{ICD}(t), \beta_{CR}(t), \beta_{ICD}(t))$, $\mathbf{s}_{micro}(t, f)=(PCD_k(t), \alpha_{PCD}(t, k), \beta_{PCD}(t, k))$, 形成时间序列 $\mathbf{timeS}(f, t)$ 和空间序列 $\mathbf{spaceS}(f, t)$, 其中 $\mathbf{timeS}_x(f, t)=(s_x(t_1, f), s_x(t_2, f), \dots, s_x(t_n, f))$, $\mathbf{spaceS}_x(f, t)=(s_x(t, f_1), s_x(t, f_2), \dots, s_x(t, f_n))$, $x \in \{\text{macro}, \text{micro}\}$, 进行 3 种主要的序列化分析: 极大极小值分析 $\arg\text{Max } \mathbf{timeS}_x(f, t)$, $\arg\text{Max } \mathbf{spaceS}_x(f, t)$, $\arg\text{Min } \mathbf{timeS}_x(f, t)$, $\arg\text{Min } \mathbf{spaceS}_x(f, t)$; 平稳性分析 $\text{Cor}(\mathbf{timeS}_x(f, t))$, $\text{Cor}(\mathbf{spaceS}_x(f, t))$; 相似性分析 $\text{Clustering}(\mathbf{timeS}_x(f, t))$, $\text{Clustering}(\mathbf{spaceS}_x(f, t))$, 及上述分析的关联性分析. 本文使用符号即含义见表 2.

本文设置攻击频率包含 5 种 (f_1, f_2, \dots, f_5), 信号灯规划算法会在每个 stage 开始前采集路口车流信息, 因此 stage 是攻击者可观测的. 攻击车辆会在每个 stage 开始前出现在路口的车辆队列末尾, 也就是 Chen 等人^[5]工作中的实验攻击频率, 在本文中将其作为基线标准, 即攻击频率 f_1 , 攻击间隔为 1 个 stage. 降频的量化是根据 stage 来调整的, 本文工作中主要选取了 4 个整数倍, 攻击车辆的攻击间隔为 stage 的 2、3、4、5 整数倍, 即频率 (f_2, f_3, f_4, f_5). 因此, 攻击频率表示为 $f=1/(k \times \text{stage})$, $k=1, 2, 3, 4, 5$, 其中 k 越大, 攻击频率 f 越小.

实际上对降频的量化可以是 stage 的整数倍也可以是非整数倍, 而非整数倍的攻击效果可以落在整数倍区间里. 例如攻击间隔为 stage 的 1.5 倍时, 与 3 倍是一样的效果, 原因是在第 1 次 1.5 个 stage 攻击时, 由于不在 stage 开始前, 攻击车辆不会被采集到, 因此是无效攻击, 而第 2 次 1.5 个 stage 攻击时, 距上一次有效攻击间隔了 3 个 stage. 为 stage 的 2.5 倍时, 与 5 倍是一样的效果, 以此类推. 因此, 本文工作选取了攻击间隔为 stage 的整数倍作为攻击频率.

表 2 符号约定

名称	描述
M	最晚到达时间阈值, $M=130$
C	平均车辆长度
$T_i, i \in [0, M]$	车辆从当前位置达到停止杆的时间
$N_j, (i \in [0, M], j \in [1, 8])$	在相位 $ph=j$, 有 N_j 辆车将会在 T_i 秒内到达停止杆
N_k	相位 $ph=k$ 上的车辆数
L_{q1}, L_{q2}	最后停止的联网车辆与倒数第 2 辆停止的联网车辆距停止杆的距离
$ph \in [1, 8]$	红绿灯相位
f	攻击频率, 规划阶段的正整数倍
$CR(t)$	t 时刻路口车辆容积率
$PCD_{ph}(t)$	t 时刻第 ph 相位的拥堵度
$ICD(t)$	t 时刻路口拥堵度
$C_k^{\max}, C_{\text{total}}^{\max}$	相位 $ph=k$ 的最大车容量, 路口最大车容量
Q_k, Q_{normal}	相位 $ph=k$ 的排队车辆数, 正常允许的排队车辆数
\mathbf{f}	频率向量
$\mathbf{s}_{macro}(t, f)$	t 时刻/频率下的宏观态势向量
$\mathbf{s}_{micro}(t, f)$	t 时刻/频率下的微观态势向量
$\mathbf{timeS}(f, t)$	频率固定的时间序列
$\mathbf{spaceS}(f, t)$	时刻固定的空间序列
$\arg\text{Max}, \arg\text{Min}$	极值计算
$\text{Cor}()$	平稳性计算函数
$\text{Clustering}()$	聚类函数

2.2 整体模型

面向攻击的态势量化分析整体框架如图 4 所示, 其中态势感知主要分为 3 个层次: 感知、理解和分析, 与该领域经典的 Endsley^[14]模型思路是一致的. Level1 感知包含容积率感知 (CR)、拥堵度感知 (ICD, PCD)、攻击加速度 ($\alpha_{CR}(t)$, $\alpha_{PCD}(t, k)$, $\alpha_{ICD}(t)$)、攻击放大比 ($\beta_{CR}(t)$, $\beta_{PCD}(t, k)$, $\beta_{ICD}(t)$); Level2 理解需要获得宏观态势向量 (s_{macro})、微观向量 (s_{micro})、时间序列 ($timeS$)、空间序列 ($spaceS$); Level3 分析涉及极大值分析 ($\arg\text{Max}timeS_x(f, t)$, $\arg\text{Max}spaceS_x(f, t)$)、极小值分析 ($\arg\text{Min}timeS_x(f, t)$, $\arg\text{Min}spaceS_x(f, t)$)、平稳性分析 ($\text{Cor}(timeS_x(f, t))$, $\text{Cor}(spaceS_x(f, t))$)、相似性分析 ($\text{Clustering}(timeS_x(f, t))$, $\text{Clustering}(spaceS_x(f, t))$) 以及关联性分析. 根据上述串行数据流的结果, 参数调整模块通过控制流对攻击定时器 f 、COP 算法的 stage 参数、针对车路环境的采集定时器 Δt , 进行相应调整. 最终实现 I-SIG 运行及车路环境反馈、变频污染攻击、3 个层次的态势感知、参数调整的闭环迭代量化分析过程.

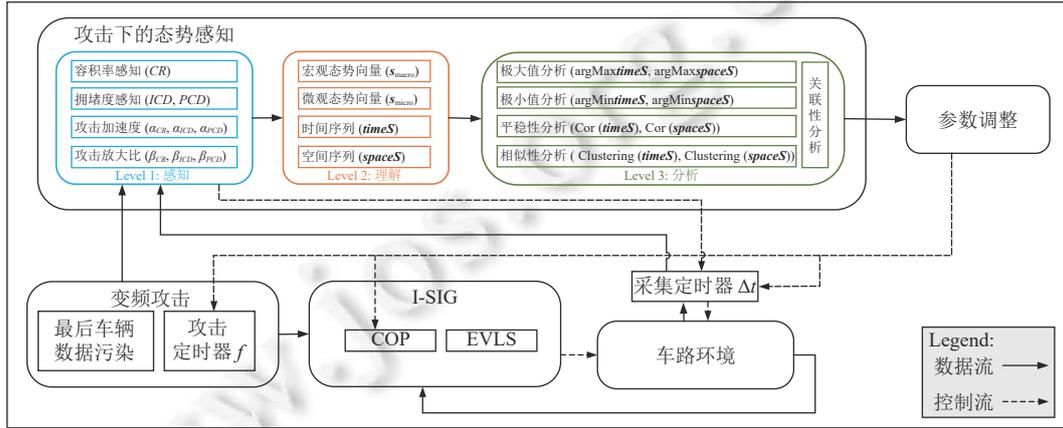


图 4 攻击下的态势量化分析整体框架图

2.3 时空序列张量构建

图 5 所示为时空序列的三阶张量 $A \in R^{I \times J \times K}$, $A_{i,j,k}$ 为张量 A 中坐标为 (i, j, k) 的元素, 其中, I, J, K 分别为向量 t, x, f 的长度 $|t|, |x|, |f|$, 属性向量 x 是具有 30 维特征的样本集合, 特征维度 $(x_1, \dots, x_{30}) = (CR(t), ICD(t), \alpha_{CR}(t), \alpha_{ICD}(t), \beta_{CR}(t), \beta_{ICD}(t), PCD(t, 1), \dots, PCD(t, 8), \alpha_{PCD}(t, 1), \dots, \alpha_{PCD}(t, 8), \beta_{PCD}(t, 1), \dots, \beta_{PCD}(t, 8))$. 将张量 A 沿采样时刻 t 展开后得到矩阵为:

$$A_{(t)} = \begin{bmatrix} A_{1,j,k} \\ A_{2,j,k} \\ \dots \\ A_{|t|,j,k} \end{bmatrix}, A_{1,j,k} = (A_{1,1,1}, A_{1,1,2}, \dots, A_{1,1,|f|}, A_{1,2,1}, \dots, A_{1,2,|f|}, \dots, A_{1,|x|,1}, \dots, A_{1,|x|,|f|}) \quad (1)$$

矩阵 $A_{(t)}$ 的每行为采样时刻 t 固定, 采样频率 f 变化的 30 个属性空间序列, 如 $(A_{1,1,1}, A_{1,1,2}, \dots, A_{1,1,|f|})$ 为第 1 个时刻第 1 个属性的空间序列, $(A_{1,|x|,1}, \dots, A_{1,|x|,|f|})$ 为第 1 个时刻第 30 个属性的空间序列.

同理, 分别将张量 A 沿属性 x 、频率 f 展开后得到的矩阵 $A_{(x)}$ 、 $A_{(f)}$ 为:

$$A_{(x)} = \begin{bmatrix} A_{i,1,k} \\ A_{i,2,k} \\ \dots \\ A_{i,|x|,k} \end{bmatrix}, A_{i,1,k} = (A_{1,1,1}, A_{2,1,1}, \dots, A_{|t|,1,1}, A_{1,1,2}, \dots, A_{|t|,1,2}, \dots, A_{1,1,|f|}, \dots, A_{|t|,1,|f|}) \quad (2)$$

$$A_{(f)} = \begin{bmatrix} A_{i,j,1} \\ A_{i,j,2} \\ \dots \\ A_{i,j,|f|} \end{bmatrix}, A_{i,j,1} = (A_{1,1,1}, A_{2,1,1}, \dots, A_{|t|,1,1}, A_{1,2,1}, \dots, A_{|t|,2,1}, \dots, A_{1,|x|,1}, \dots, A_{|t|,|x|,1}) \quad (3)$$

矩阵 $A_{(f)}$ 的每行为采样频率 f 固定, 采样时刻 t 变化的 30 个属性的时间序列, 如 $(A_{1,1,1}, A_{2,1,1}, \dots, A_{|t|,1,1})$ 为第 1 种频率下第 1 个属性的时间序列, $(A_{1,|x|,1}, \dots, A_{|t|,|x|,1})$ 为第 1 种频率下第 30 个属性的时间序列。

第 t 个时刻的空间序列和第 f 种频率下的时间序列分别表示如下:

$$\text{spaceS}(f, t) = \{A_{i,j,f} | i = t \in [1, |t|], j \in [1, 30]\} = \{A_{t,1,:}, A_{t,2,:}, \dots, A_{t,30,:}\},$$

$$\text{timeS}(f, t) = \{A_{t,j,k} | j \in [1, 30], k = f \in [1, |f|]\} = \{A_{:,1,f}, A_{:,2,f}, \dots, A_{:,30,f}\},$$

其中, $A_{i,j,:}$ 表示第 i 个时刻第 j 个属性在不同攻击频率下的空间序列, $A_{:,j,k}$ 表示第 k 种频率下第 j 个属性在不同采样时刻的时间序列。最终得到 $30 \times |t|$ 个空间序列和 $30 \times |f|$ 个时间序列分别为: $\cup_{f=1}^{|f|} \text{spaceS}(f, t)$, $\cup_{t=1}^{|t|} \text{timeS}(f, t)$ 。

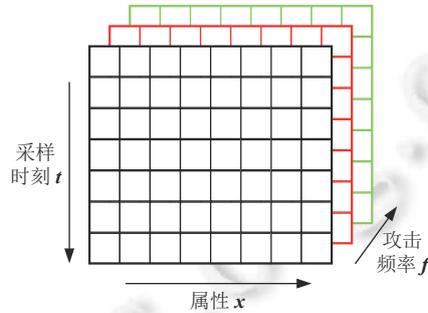


图 5 时空序列的三阶张量 A 示意图

2.4 极大极小值分析

极大极小值分析, 一方面需要在三阶张量 A 的某个属性 x 切面中, 寻找极大极小值; 另一方面, 需要分别记录取得该极值的时刻 t 值与频率 f 值, 如算法 1 所示。

算法 1. $\text{MaxMinCompute}(A)[x]$.

输入: 时空序列的三阶张量 A ;

输出: 属性极值向量 $(\text{MaxMinCompute}(A)[1], \dots, \text{MaxMinCompute}(A)[|x|])$, 其中 $\text{MaxMinCompute}(A)[x] = (\text{Max}, t_max, f_max, \text{Min}, t_min, f_min)$.

1. for each $x \in x$:
2. $\text{Max} = \max_{i,k} A_{i,x,k}$; // 求 x 切面极大值
3. $t_max = \arg \max_i A_{i,x,k}$; $f_max = \arg \max_k A_{i,x,k}$;
4. $\text{Min} = \min_{i,k} A_{i,x,k}$; // 求 x 切面极小值
5. $t_min = \arg \min_i A_{i,x,k}$; $f_min = \arg \min_k A_{i,x,k}$;
6. $\text{MaxMinCompute}(A)[x].\text{add}(\text{Max}, t_max, f_max, \text{Min}, t_min, f_min)$;
7. end for
8. return $\text{MaxMinCompute}(A)[x]$

算法 1 中, 第 2 行得到第 x 维属性的切面 $A_{i,x,k}$ 中的极大值 Max , 进而计算极大值时所对应的时刻 t_max 和频率 f_max ; 同理, 第 4, 5 行获得极小值时所对应的时刻 t_min 和频率 f_min 。

2.5 平稳性分析

平稳性分析主要用来考察在固定某个频率 f 下属性 x 的值随时间变化的稳定性, 可通过计算序列的自相关函数进行对比分析。算法 2 针对某属性 x 在三阶张量 A 中的属性切面, 提供不同频率 f 下的时间序列的自相关系数^[15]计算。

算法 2. $CorCompute(A_{i,x,k})[f]$.

输入: 第 x 维属性的切面 $A_{i,x,k}$, 最大对比间隔 w ;

输出: 自相关系数向量 ($CorCompute(A_{i,x,k})[1], \dots, CorCompute(A_{i,x,k})[f]$).

1. for each $k \in [1, |f|]$:
2. for each $n \in [1, N]$:
3. $Cor = \sum_{i=0}^{|l|-n} (A_{i,x,k} - \overline{A_{i,x,k}})(A_{i+n,x,k} - \overline{A_{i,x,k}}) / \sum_{i=0}^{|l|} (A_{i,x,k} - \overline{A_{i,x,k}})^2$
4. $CorCompute(A_{i,x,k})[f].add(Cor)$;
5. end for
6. end for
7. return $CorCompute(A_{i,x,k})[f]$

算法 2 可以看出, 针对第 x 维属性切面 $A_{i,x,k}$ 中的时间序列, 利用第 3 行的自相关系数输出自相关系数向量.

2.6 相似性分析

在相似性分析方面, 主要采用 AGNES 层次聚类法. 尽管层次聚类法可能会遇到合并或分裂点选择的困难, 影响聚类质量, 但在实验分析中, 可通过层次聚类树状图及分割层实现可视化、可解释的聚类及优化调整. 针对不同时刻不同频率下的属性序列, 通过聚类 (如算法 3 所示) 寻找相似的序列向量, 其中属性序列相似度计算公式如下:

$$d(A_{i,x,k}, A_{i',x,k'}) = \sqrt{(A_{i,x,k} - A_{i',x,k'})^T S^{-1} (A_{i,x,k} - A_{i',x,k'})} \quad (4)$$

其中, S 为 $A_{i,x,k}$ 和 $A_{i',x,k'}$ 的协方差矩阵.

算法 3. $seqClustering(A_{i,x,k})$.

输入: 属性序列集 $\{A_{i,x,k} | i \in |I|, k \in |f|\}$, 终止簇的数目 K ;

输出: K 个相似簇.

1. $C = \{A_{i,x,k} | i \in |I|, k \in |f|\}$;
2. for each $p \in [1, |C|]$:
3. for each $q \in [1, |C|]$:
4. $d_{avg}(C_p, C_q) = \frac{1}{|C_p||C_q|} \sum_{b \in C_p} \sum_{h \in C_q} d(b, h)$; // 平均距离 d_{avg}
5. $M_{p,q} = d_{avg}(C_p, C_q)$;
6. end for
7. end for
8. $c = |C|$;
9. while $c > K$:
10. $p, q, min = findMin(M)$; // 找出距离最近的两个聚类簇 C_p 和 C_q , $min_{p,q}$ 为最小聚类簇距离
11. $C_p.extend(C_q)$;
12. $C.remove(C_q)$;
13. for each $p \in [1, |C|]$:
14. for each $q \in [1, |C|]$:
15. $d_{avg}(C_p, C_q) = \frac{1}{|C_p||C_q|} \sum_{b \in C_p} \sum_{d \in C_q} d(b, d)$;
16. $M_{p,q} = d_{avg}(C_p, C_q)$;

```

17.   end for
18.   end for
19.  $c = c - 1$ ;
20. return  $C$ 

```

算法 3 中第 1 行将所有的属性序列看作一个初始聚类簇并放入集合 C 中, 第 2–7 行计算 C 中任意两个簇之间的距离, 并存入 M 中, 其中两个簇的距离采取平均距离的计算, 两个属性序列相似性采用马氏距离 (如公式 4 所示); 第 8 行设置当前的聚类数目为 $|C|$ 个; 当前聚类数目大于终止簇数目 K 时, 第 9–19 行执行循环聚类操作; 第 10 行计算找出距离最近的两个聚类簇 C_p 和 C_q , 且 $\min_{p,q}$ 为最小聚类簇的距离; 第 11, 12 行将集合 C_p 和 C_q 合并, 赋值给 C_p , 并在集合 C 中删除 C_q ; 第 13–18 行根据更新后的集合 C , 更新距离矩阵 M .

2.7 关联性分析

关联性分析以极大极小值为触发点, 对三阶张量空间 A 中所有的极大极小值点进行时间序列 $A_{t,j,k} \in \cup_{f=1}^n \text{timeS}(f, t)$ 和属性序列 $A_{i,x,k}$ 的提取, 进行 3 种操作: 1) 对时间序列 $A_{t,j,k}$ 进行平稳性分析; 2) 分析属性序列 $A_{i,x,k}$ 是否落入相同的聚类; 3) 分析同一个聚类簇下属性序列对应的时间频率分布 $\text{Distri}(t, f)$. 关联分析算法中的函数依赖关系如图 6 所示, 具体调用细节如算法 4 所示.

算法 4. void *CorreAna*(A).

输入: *MaxMinCompute*(A)[x], *seqClustering*($A_{i,x,k}$);

输出: 3 种操作.

```

1. for each  $x \in [1, |x|]$ :
2.    $Max, t\_max, f\_max, Min, t\_min, f\_min = \text{MaxMinCompute}(A)[x]$ ;
3.    $Cor_1.add(\text{CorCompute}(A_{i,x,k})[f\_max])$ ;
4.    $Cor_2.add(\text{CorCompute}()[f\_min])$ ;
5.   Do  $Comp(Cor_1, Cor_2)$ ; // 平稳性对比
6.   for  $(i, k)$  in  $\{(t\_max, f\_max), (t\_min, f\_min)\}$ :
7.     find  $A_{i,x,k}$  in  $seqClustering(A_{i,x,k})$ ;
8.     get  $A_{i,x,k}$  属于的聚类  $C$ , 加入对比集合  $C'$ ;
9.     Do  $Distri(t, f)$ ;
10.  end for
11. end for
12. Do  $Comp(C')$ ; // 聚类对比
13. return

```

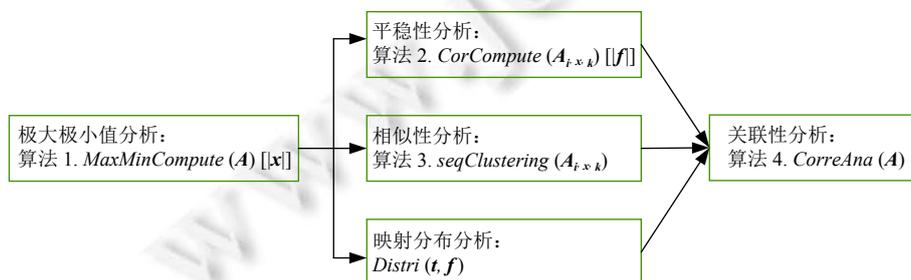


图 6 关联分析算法中的函数依赖关系图

算法 4 中, 第 2 行调用 $MaxMinCompute(A)[|x|]$ 计算属性 x 切面中的极大极小值 (Max, Min) 及其所对应的时刻和频率 ($t_{max}, f_{max}, t_{min}, f_{min}$), 第 3, 4 行调用 $CorCompute(A_{i,x,k})[|f|]$ 计算频率 f_{max} 和 f_{min} 下时间序列的自相关系数序列; 第 5 行对利用第 3, 4 行所得到的序列对时间序列进行平稳性分析; 第 7, 8 行调用 $seqClustering(A_{i,x,k})$ 对极大极小值点所属的属性序列进行聚类分析; 第 9 行分析同一个聚类簇中属性序列的时间频率分布 $Distrib(t, f)$.

3 实验

3.1 实验设置

实验平台和实验环境配置如表 3 所示. 通过运行 COP 和 VISSIM^[16], 实现 I-SIG 信号灯控制与交通流量仿真, 为交通拥堵态势量化分析提供基础的数据采集.

表 3 实验环境配置

平台	实验环境	实验配置
COP & VISSIM	操作系统	Windows 10
	CPU	AMD Ryzen5 3550H with Radeon Vega Mobile Gfx 2.10 GHz
	RAM	16 GB
	软件	PTV Vissim 4.30, Visual Studio 2019

3.2 实验设计

如图 7 所示, COP 算法规划的红绿灯变化及车流量变化都可以被 VISSIM 实时地捕捉和展现. 除了可视化分析, 本文实现了从 VISSIM 到时空序列三阶张量的自动数据采集与存储. 其中, 变频攻击主要通过 1800 s 的循环迭代实现, 实验频率主要包含 5 种 (f_1, f_2, \dots, f_5), 分别对应添加攻击车辆间隔为 stage 的 1、2、3、4、5 整数倍. 实际上, f_1 为 Chen 等人^[5]工作中的实验攻击频率, 在本文中作为基线标准.

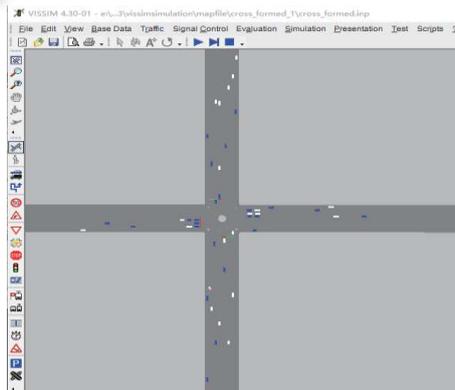


图 7 VISSIM 仿真环境图

本实验设计中, 考察路口范围为红绿灯 300 m 内, 不考虑右转车道的情况下, 包括东西南北 4 个方向的直行和左转共 8 个红绿灯相位, 车辆的长度为 4.11–4.76 m. 本实验设计的采样时间间隔为 20 s.

3.3 实验结果及分析

在本节中, 基于时空序列三阶张量 A , 首次系统性地开展了变频污染攻击的智能交通拥堵态势量化分析, 主要涉及极大极小值分析、平稳性分析、相似性分析以及关联性分析.

(1) 极值分析

如表 4 所示, 给出了 12 种典型属性的极大极小值及相应的时刻与频率 (t, f), 其中宏观属性包括 ($CR, ICD, \alpha_{CR}, \alpha_{ICD}, \beta_{CR}, \beta_{ICD}$), 微观属性包括 ($PCD(3), \alpha_{PCD}(3), \beta_{PCD}(3), PCD(4), \alpha_{PCD}(4), \beta_{PCD}(4)$).

表 4 特征极值表

极大极小值	宏观属性						微观属性					
	x_1 CR	x_2 ICD	x_3 α_{CR}	x_4 α_{ICD}	x_5 β_{CR}	x_6 β_{ICD}	x_9 $PCD(3)$	x_{17} $\alpha_{PCD(3)}$	x_{25} $\beta_{PCD(3)}$	x_{10} $PCD(4)$	x_{18} $\alpha_{PCD(4)}$	x_{26} $\beta_{PCD(4)}$
Max	0.4233	14.2	0.0022	0.0567	254.0	104.0	2.6	0.0093	26.0	1.7	0.0125	17
$t(Max)$	1382	1342	2	22	1342	1722	762	102	762	102	2	102
$f(Max)$	1	1	3	3	1	4	1	3	1	3	1	3
Min	0.0617	1.5	0.0001	0.0012	37.0	7.5	0.0	0.0	0.0	0.0	0.0	0.0
$t(Min)$	2	2	1602	1742	2	2	2	2	2	22	22	22
$f(Min)$	5	5	5	5	5	5	1	1	1	1	1	1

由于属性量纲不一致, 其中属性 ($ICD, \beta_{CR}, \beta_{ICD}, PCD(3), \beta_{PCD(3)}, PCD(4), \beta_{PCD(4)}$) 的极大值均超过 1, 分别为 (14.2, 254.0, 104.0, 2.6, 26.0, 1.7, 17). 可以看出, 极大值均未出现在最后时刻, 最大攻击频率 f_1 在靠后的时刻在属性 (CR, ICD, β_{CR}) 上产生极大值, 而降频 f_3 和 f_4 会在中间靠前的时刻在属性 ($\alpha_{CR}, \alpha_{ICD}, \alpha_{PCD(3)}, PCD(4), \beta_{PCD(4)}$) 上产生极大值, 说明降频攻击仍然有效. 但是, 最大降频 f_5 会造成宏观属性的非零最小值, 而微观属性的最小值可以达到 0.

图 8 给出了 12 种特征值标准化后的箱图, 便于观察值分布. 可以看出, 属性 ($x_1, x_2, x_5, x_6, x_9, x_{25}$) 特征值总体分布均匀; 属性 (x_{10}, x_{26}) 不存在下边界, 而属性 (x_3, x_4, x_{17}, x_{18}) 特征值分布不均匀, 出现了较多的异常点, 说明值空间中较大值数量较多.

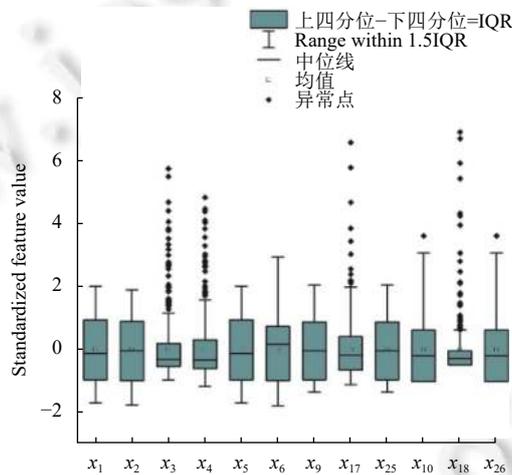


图 8 特征值标准化箱图

(2) 平稳性分析

针对宏观属性 CR 与 ICD 的平稳性分析如图 9 和图 10 所示, 图 9 为特征值时序图, 图 10 为自相关对比图. 如图 9 所示, f_1-f_5 不同频率下 CR 与 ICD 特征值均会随着时间变化上下跳动, f_1-f_4 呈现一般上升趋势, 而 f_5 频率下 CR 与 ICD 特征值全局趋势平稳, 细节数据可参加图 10 中的红框, 可以看出 f_5 自相关系数, 在零周围波动, CR, ICD 自相关系数波动序列分别为 $(-0.027, 0.045, -0.011, 0.066, 0.040, 0.096, 0.062, 0.079, -0.001, 0.001, -0.061), (0.033, -0.012, 0.034, 0.089, -0.068, -0.098, -0.035, 0.023, 0.008, -0.037, 0.071, 0.029, -0.115)$, 没有明显的收敛趋势, 数据序列全局相对平稳的.

(3) 相似性与关联分析

如表 5 所示, 对张量空间中 450 个属性序列进行聚类, 聚类数设置为属性序列数的 3%~5% ($|C|=13\sim 22$). 从簇内元素数可以看出, 聚类簇的元素数不均衡, 存在个别簇元素数超过 50%, 例如 $|C|=13$ 时, $|C_9|=296, |C|=22$ 时, $|C_{13}|=235$. 簇间平均距离与最小簇内平均距离对比明显, 说明聚类算法是有效的.

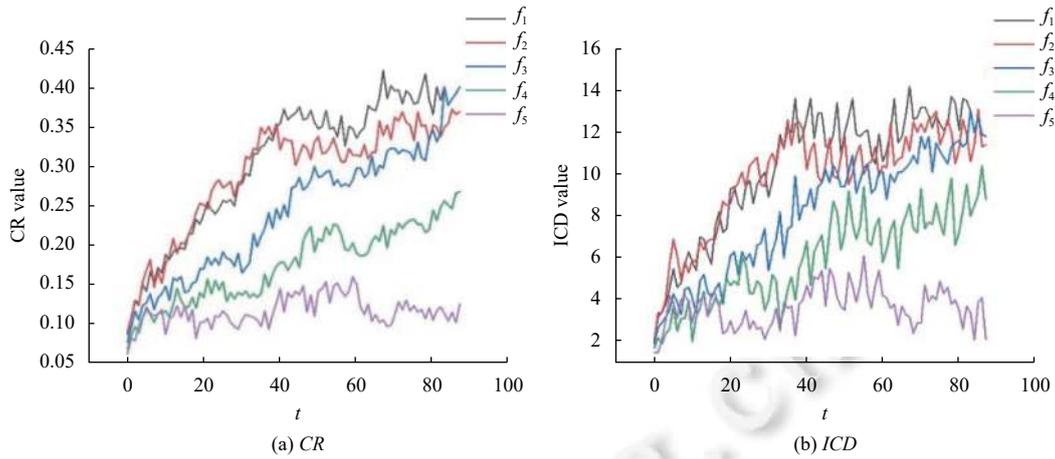


图9 特征值时序图

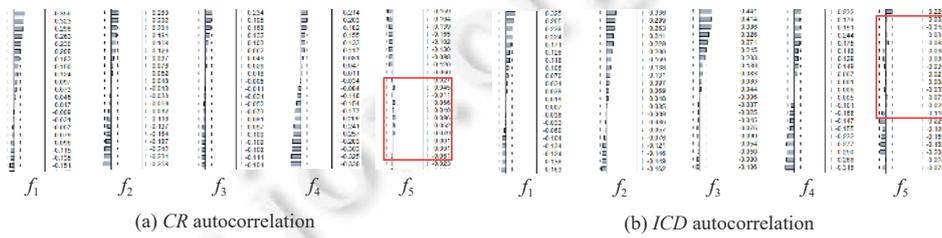


图10 自相关对比图

表5 聚类结果表

聚类数 $ C $	簇内元素数	簇间平均距离 $ C \geq 1$	最小簇内平均距离 $ C \geq 2$
13	(6, 2, 2, 5, 3, 1, 4, 101, 296, 9, 17, 3, 1)	9.9633	3.6720
14	(3, 3, 2, 2, 5, 3, 1, 4, 101, 296, 9, 17, 3, 1)	9.8594	3.5684
15	(3, 3, 2, 2, 5, 3, 1, 4, 101, 289, 7, 9, 17, 3, 1)	9.6411	3.5684
16	(3, 3, 2, 2, 5, 3, 1, 4, 101, 289, 7, 8, 17, 3, 1, 1)	9.5837	3.5684
17	(54, 3, 3, 2, 2, 5, 3, 1, 4, 101, 235, 7, 8, 17, 3, 1, 1)	9.2312	3.5684
18	(54, 3, 3, 2, 2, 5, 3, 1, 4, 89, 12, 235, 7, 8, 17, 3, 1, 1)	9.2785	3.5684
19	(26, 3, 3, 2, 2, 5, 3, 1, 28, 4, 89, 12, 235, 7, 8, 17, 3, 1, 1)	8.9577	3.4690
20	(26, 3, 3, 2, 2, 5, 3, 1, 28, 4, 89, 12, 235, 5, 8, 2, 17, 3, 1, 1)	8.8465	3.4690
21	(26, 3, 3, 2, 2, 5, 3, 1, 28, 4, 89, 12, 235, 5, 8, 2, 12, 5, 3, 1, 1)	9.2358	3.4690
22	(26, 3, 3, 2, 2, 5, 3, 1, 28, 4, 74, 12, 235, 5, 15, 8, 2, 12, 5, 3, 1, 1)	9.2340	3.4690

挑选 $|C|=13$ 中的簇 C_9 与 $|C|=22$ 的簇 C_{13} 进行细粒度的时间频率分布对比,如图11所示,可以看出 C_9 、 C_{13} 分别作为最大簇,投影在不同频率上的时间分布大体相似,随着频率的降低,相似属性序列数目增加,且随时间递增,相似序列集中.如图中蓝色与红色矩形框所示,同一个属性序列分别出现在 $|C|=13$ 中的簇 C_9 和 $|C|=22$ 的簇 C_{13} 中,对应 f_3 频率下的 $t=102$ 时刻,而此时该序列中存在2个属性的最大值,分别为 $\alpha_{PCD}(3)=0.0093$ 、 $PCD(4)=1.7$,对应关联如图中虚线箭头所示.

综上实验分析,除细节数据结果外,可得到两个较为明显的宏观结果:(1)降频攻击(f_2, f_3, f_4, f_5)仍然可产生明显的攻击效果;(2)降频下容积率和拥堵度具有更稳定的自相关系数表征.

3.4 不同分析方法的关联关系讨论

通过极值分析可以对比不同特征值的极大极小值会出现在不同攻击频率下会出现在什么时间,从而分析不同

攻击频率所产生的攻击效果, 低攻击频率下极大值更小. 通过平稳性分析, 可以判断不同频率下特征值随时间变化的波动状态, 同时根据自相关系数的收敛趋势, 也可以判断特征时间序列的平稳性, 低攻击频率下的时间序列更平稳. 通过特征序列相似性分析, 可以得到不同频率下特征序列相似的数目以及相似序列集中的时间段, 低攻击频率下相似序列数目更多, 时间上也更集中.

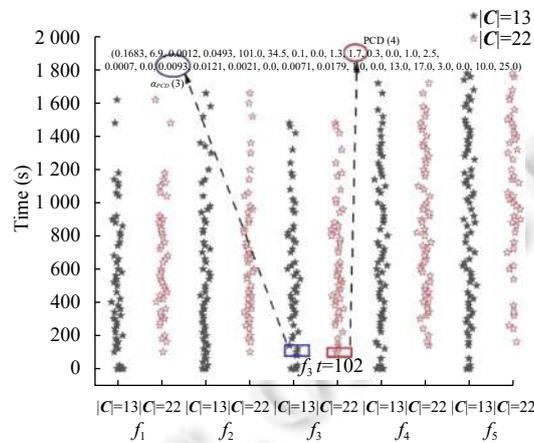


图 11 最大簇的时间频率分布对比图

3 种分析在逻辑上是相互依赖的, 几种分析之间是紧密关联的, 为拥堵态势分析提供了初步支撑, 并且这 3 种分析目前是迫切的, 随着拥堵态势分析需求的增加, 还有更多的分析方法可以扩展进来.

通过采集路口车流量, 对攻击效果进行量化, 利用量化后的不同特征, 通过一体化分析方法从不同维度来分析不同攻击频率特征的变化, 从而分析攻击频率对攻击效果的具体影响. 针对不同频率的数据污染攻击, 所提出的基于函数依赖关系 3 种分析相关联的一体化分析, 能够较全面地对数据污染攻击下的 I-SIG 路口的交通数据作不同维度的分析, 也为后续防御不同频率的数据污染攻击的自动化实现提供了支撑.

3.5 单路口与多路口应用讨论

智能交通信号灯控制系统 I-SIG 的特点是单路口应用, 作为车联网的一部分, 已经开始在美国试点. 本文针对单个 I-SIG 路口场景下提出的拥堵态势感知量化分析的方法, 对于乡镇和非人口密集城市等区域, 具有较大的应用范围.

而对于人口密集城市, 通过对多个单路口的分析, 可以为多路口的拥堵态势分析提供统计上的简单判断. 但是由于一定范围内的多个 I-SIG 路口之间交通状况的复杂性, 某些路口的车流量和拥堵情况会对其他路口产生影响, 从而影响整个区域的拥堵程度, 对于进一步的多路口拥堵态势协同判断, 单路口的拥堵态势量化分析在多路口场景下存在一定的局限性和不足.

局限性及未来工作的改进方向如下.

(1) 对于单路口的拥堵态势分析, 感知层包括容积率感知 (CR)、拥堵度感知 (ICD , PCD)、攻击加速度感知 (α_{CR} , α_{ICD} , α_{PCD})、以及攻击放大比感知 (β_{CR} , β_{ICD} , β_{PCD}) 等拥堵指标的计算, 这些拥堵指标是基于单个路口的拥堵程度提出的, 因此, 要衡量多个路口的拥堵程度, 未来我们需要基于多个单路口的拥堵指标设计新的感知层的拥堵指标计算方法.

(2) 由于一个区域内的多个路口之间的关联性, 如图 12 所示为多路口场景, 该场景包含了 3 个 I-SIG 路口, 分别为 R_1 , R_2 , 和 R_3 , 路口 R_2 是路口 R_1 的 4 相位、5 相位车流和路口 R_3 的 1 相位、8 相位车流的后必经路口, 会对 R_2 的拥堵情况产生关联影响. 因此, 未来我们会从相位的粒度建立路口间的关联图, 进一步进行多路口拥堵态势协同分析.

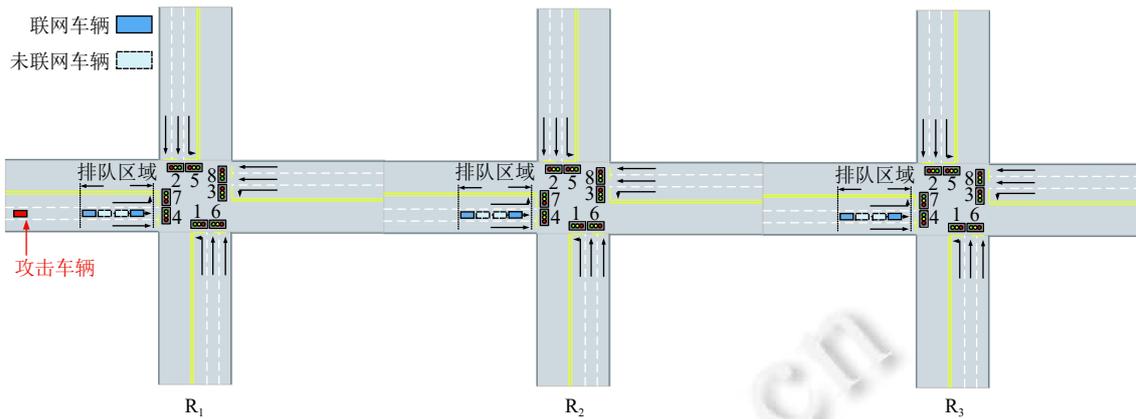


图 12 多路口场景图

4 相关工作与比较

智能交通系统中的数据污染攻击存在多种形式. 针对车辆来说, 已经发现了针对麦克风传感器、超声波传感器、雷达传感器、车载摄像头等的攻击. 在针对麦克风传感器攻击的相关工作中, 研究人员发现了 *Dolphin-Attack*^[17] 攻击, 该攻击可以利用人类无法听到的高频声音, 对智能设备的语音助手发出命令并操作其工作. 通过变频后的超声波信号, 几乎可以操作市场上主流的包括 Siri, Google Now, Huawei HiVoice 在内的语音识别系统和奥迪汽车的语言控制导航系统. Liu 等人^[18] 开展了针对特斯拉的超声波传感器进行干扰和攻击的实验, 通过使用简单的 Arduino Uno 板产生 40 kHz 的超声波, 并向汽车传感器连续发射以降低其信噪比, 在超声波攻击信号与传感器侧的原始信号重叠的干扰攻击下, 传感器无法检测到周围的障碍物. 对雷达传感器的攻击研究中, 研究人员使用高精度的信号分析仪识别出特斯拉雷达传感器的频率, 然后产生相同频率的电磁波来干扰和欺骗雷达系统, 或者是将谐波混频器的信号转发到发射器, 然后再发送回雷达以模拟更远的目标, 采用中继信号紧跟着真实信号的伪装方法, 当打开雷达干扰时, 汽车雷达系统检测到汽车并显示, 而当关闭干扰时汽车立即消失^[19], 从而在自动驾驶的过程中造成雷达系统检测出错.

而目前发现的 I-SIG 规划系统中的数据污染攻击, 主要是针对规划系统实施, 污染攻击属于获得权限后的主动数据污染, 例如 Chen 等人^[5] 通过修改装配车辆的速度和位置信息, 伪装成迟到的“幽灵车辆”, 实现对信号灯规划算法 COP 的漏洞攻击. 本文研究范畴也属于该类数据污染攻击, 是主动发送错误数据攻击规划系统, 而非针对传感器层面的间接攻击, 因此可以调节攻击的频率. 此外, 已有工作聚焦的是端到端的攻击效果分析, 并未在方法和实验上呈现过程性的全时序拥堵态势分析, 而本文是针对单路口 I-SIG 系统首次开展降频攻击的全时序实验分析.

5 结论

在单路口智能交通系统 I-SIG 中, 本文针对降频数据污染攻击, 首次在方法和实验上分析了过程性的全时序拥堵态势, 发现了新的实验结果, 包括降频攻击仍然可产生明显的攻击效果、低频下容积率和拥堵度具有更稳定的自相关系数表征, 为自动化防御的工程实现提供了支持. 本文提出一种面向多个降频污染攻击的统一拥堵态势量化与分析框架, 通过正交攻击频率维、攻击相关空间特征维与时序维, 构建了时空序列的三阶张量空间, 能针对性地服务于 I-SIG 在持续攻击状态下的单路口拥堵态势感知; 进一步基于函数依赖关系设计 3 种具体分析相关联的一体化分析方法, 包括基于张量的极值分析、基于自相关的平稳性分析、基于不同聚类簇的关联性分析. 在交通模拟环境 VISSIM 平台, 开展了 5 种攻击频率下的 30 分钟流量对比, 系统地报告了量化分析的结果. 由于 I-SIG 在实际应用中会部署在多个路口, 因此, 如何面向协同的降频攻击及其带来交通流量冲击仍需进一步研究, 并在实践中进一步扩展与完善.

References:

- [1] Zhu L, Yu FR, Wang YG, Ning B, Tang T. Big data analytics in intelligent transportation systems: A survey. *IEEE Trans. on Intelligent Transportation Systems*, 2019, 20(1): 383–398. [doi: [10.1109/TITS.2018.2815678](https://doi.org/10.1109/TITS.2018.2815678)]
- [2] U. S. Department of Transportation. USDOT: Multi-modal intelligent traffic safety system (MMITSS). 2020. https://www.its.dot.gov/research_archives/dma/bundle/mmitss_plan.htm
- [3] U. S. Department of Transportation. U. S. dot connected vehicle pilot deployment program. 2020. <https://www.its.dot.gov/pilots/>
- [4] U. S. Department of Transportation. Connected vehicle applications. 2020. https://www.its.dot.gov/pilots/cv_pilot_apps.htm
- [5] Chen QA, Yin YC, Feng YH, Mao ZM, Liu HX. Exposing congestion attack on emerging connected vehicle based traffic signal control. In: *Proc. of the Network and Distributed Systems Security Symp.* San Diego: The Internet Society, 2018. 1–15. [doi: [10.14722/ndss.2018.23222](https://doi.org/10.14722/ndss.2018.23222)]
- [6] Wang XJ, Xiang YX, Wen WJ, Tong ED, Chen QA, Li G, Liu JQ, Li L. Constructing optimal sparse decision tree for analyzing I-SIG system attack. In: *Proc. of the 2020 IEEE Int'l Conf. on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCLOUD/SocialCom/SustainCom)*. Exeter: IEEE, 2020. 321–328. [doi: [10.1109/ISPA-BDCLOUD-SocialCom-SustainCom51426.2020.00066](https://doi.org/10.1109/ISPA-BDCLOUD-SocialCom-SustainCom51426.2020.00066)]
- [7] Wang XJ, Xiang YX, Niu WJ, Tong ED, Liu JQ. Explainable congestion attack prediction and software-level reinforcement in intelligent traffic signal system. In: *Proc. of the 26th IEEE Int'l Conf. on Parallel and Distributed Systems (ICPADS)*. Hong Kong: IEEE, 2020. 667–672. [doi: [10.1109/ICPADS51040.2020.00094](https://doi.org/10.1109/ICPADS51040.2020.00094)]
- [8] Sen S, Head KL. Controlled optimization of phases at an intersection. *Transportation Science*, 1997, 31(1): 5–17. [doi: [10.1287/trsc.31.1.5](https://doi.org/10.1287/trsc.31.1.5)]
- [9] Feng YH, Head KL, Khoshmagham S, Zamanipour M. A real-time adaptive signal control in a connected vehicle environment. *Transportation Research Part C: Emerging Technologies*, 2015, 55: 460–473. [doi: [10.1016/j.trc.2015.01.007](https://doi.org/10.1016/j.trc.2015.01.007)]
- [10] U. S. Department of Transportation. US department of transportation hopes to mandate V2V communications. 2020. <https://www.cnet.com/roadshow/news/us-department-of-transportation-hopes-to-mandate-v2v-communications>
- [11] Xiong HY, Tan ZR, Zhang RH, He S. A new dual axle drive optimization control strategy for electric vehicles using vehicle-to-infrastructure communications. *IEEE Trans. on Industrial Informatics*, 2020, 16(4): 2574–2582. [doi: [10.1109/TII.2019.2944850](https://doi.org/10.1109/TII.2019.2944850)]
- [12] Kenney JB. Dedicated short-range communications (DSRC) standards in the United States. *Proc. of the IEEE*, 2011, 99(7): 1162–1182. [doi: [10.1109/JPROC.2011.2132790](https://doi.org/10.1109/JPROC.2011.2132790)]
- [13] Patel RK, Seymour EJ. The national transportation communication for ITS protocol (NTCIP) for transportation interoperability. In: *Proc. of the Conf. on Intelligent Transportation Systems*. Boston: IEEE, 1997. 543–548. [doi: [10.1109/ITSC.1997.660532](https://doi.org/10.1109/ITSC.1997.660532)]
- [14] Endsley MR. Situation awareness global assessment technique (SAGAT). In: *Proc. of the 1988 IEEE National Aerospace and Electronics Conf.* Dayton: IEEE, 1988. 789–795. [doi: [10.1109/NAECON.1988.195097](https://doi.org/10.1109/NAECON.1988.195097)]
- [15] Sanborn S, Ma X. Quantifying information content in data compression using the autocorrelation function. *IEEE Signal Processing Letters*, 2005, 12(3): 230–233. [doi: [10.1109/LSP.2004.842264](https://doi.org/10.1109/LSP.2004.842264)]
- [16] PTV Vissim. 2020. <http://vision-traffic.ptvgroup.com/en-us/products/ptv-vissim>
- [17] Zhang GM, Yan C, Ji XY, Zhang TC, Zhang TM, Xu WY. DolphinAttack: Inaudible voice commands. In: *Proc. of the 2017 ACM SIGSAC Conf. on Computer and Communications Security (CCS 2017)*. Dallas: ACM, 2017. 103–117. [doi: [10.1145/3133956.3134052](https://doi.org/10.1145/3133956.3134052)]
- [18] Yan C, Xu WY, Liu JH. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicles. *Def Con*, 2016, 24(8): 109. [doi: [10.5446/36252](https://doi.org/10.5446/36252)]
- [19] Fu K, Xu WY. Risks of trusting the physics of sensors. *Communications of the ACM*, 2018, 61(2): 20–23. [doi: [10.1145/3176402](https://doi.org/10.1145/3176402)]



相迎宵(1994-), 女, 博士生, 主要研究领域为人工智能安全.



陈彤(1993-), 女, 博士, 主要研究领域为网络空间安全.



李轶珂(1995-), 女, 博士生, 主要研究领域为智能交通, 强化学习安全.



童恩栋(1986-), 男, 博士, 讲师, CCF 专业会员, 主要研究领域为人工智能安全, 安全强化学习.



刘吉强(1973-), 男, 博士, 教授, CCF 专业会员, 主要研究领域为可信计算, 隐私保护, 网络安全.



牛温佳(1982-), 男, 博士, 教授, CCF 高级会员, 主要研究领域为人工智能安全, 数据挖掘.



王潇瑾(1997-), 女, 硕士, 主要研究领域为人工智能安全.



韩臻(1962-), 男, 博士, 教授, CCF 专业会员, 主要研究领域为计算机安全, 网络与信息安全.