计算机科学与探索
Journal of Frontiers of Computer Science and Technology
1673-9418/2024/18(02)-0516-10
doi: 10.3778/j.issn.1673-9418.2211032

面向车载自组织网络的混合信任管理方案研究

项　丹,陈泽茂+
武汉大学 国家网络安全学院 空天信息安全与可信计算教育部重点实验室,武汉 430040
+ 通信作者 E-mail: chenzemao@whu.edu.cn

摘　要:随着智能交通的快速发展,车载自组织网络(VANETs)具有广阔的发展前景,但也面临多种安全威胁。针对车载自组织网络中可能存在的内部攻击者和虚假消息,提出了一种分布式的混合信任管理方案HTMS-V。该方案考虑到车载自组织网络的特性,基于改进的主观逻辑模型结合直接信任和间接信任对网络中的车辆节点进行信任评估,基于节点间的交互记录建立节点间的信任关系;基于节点信任和节点间距离进行消息信任评估,并根据信任评估结果识别网络中的虚假消息和恶意节点。为了验证所提出方案的性能,设计了四种不同的攻击场景,在车辆网络仿真平台Veins上进行对比实验,测试HTMS-V方案在各种攻击场景下的表现。实验结果表明,HTMS-V方案能有效抵抗车载自组织网络中的各种攻击,在40%恶意节点率的情况下仍能识别大部分虚假消息和恶意节点,且HTMS-V方案的表现明显优于由主观逻辑模型和基于距离的加权投票构成的基线方案。

关键词:车载自组织网络(VANETs);信任管理;主观逻辑
文献标志码:A　**中图分类号:**TP393.08

Research on Hybrid Trust Management Scheme for VANETs

XIANG Dan, CHEN Zemao+
Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430040, China

Abstract: With the rapid development of intelligent transportation, vehicular ad hoc networks (VANETs) has broad development prospects, but also faces a variety of security threats. A distributed hybrid trust management scheme called HTMS-V is proposed for insider attackers and false message detection in VANETs. Specifically, considering the characteristics of VANETs, node trust is evaluated based on the improved subjective logic model. The evaluation combines direct trust and indirect trust, and the trust relationship between nodes is established based on interaction records. Message trust is evaluated based on node trust and the distance between nodes. And the scheme identifies false messages and malicious nodes based on the trust evaluation results. This paper tests the performance of the HTMS-V scheme under four attack scenarios. The simulation results show that the HTMS-V scheme effectively resists various attacks in VANETs and is able to identify most false messages and malicious nodes even if the malicious node ratio reaches 40%, and the performance of the HTMS-V scheme is obviously better than that of the baseline scheme which is composed of subjective logical model and distance based weighted voting.

Key words: vehicular ad hoc networks (VANETs); trust management; subjective logic

基金项目:国家自然科学基金(61872430)。
This work was supported by the National Natural Science Foundation of China (61872430).
收稿日期:2022-11-09　**修回日期:**2023-01-17

近年来，随着交通行业的快速发展，智能交通系统（intelligent transportation system，ITS）应运而生，作为ITS的一个重要组成部分，车载自组织网络（vehicular ad hoc networks，VANETs）正受到商业界和学术界的广泛关注。VANETs主要由车辆节点、路边单元（roadside unit，RSU）和可信权威机构（trusted authority，TA）构成。VANETs中通常通过车辆节点之间、车辆节点与RSU之间的通信来传播信息，以此保障道路安全与交通效率[1]。真实可靠的数据传播对于VANETs至关重要。在典型的VANETs应用场景中（如碰撞预警、道路危险状况提示、异常车辆提醒等），车辆可以接收道路上的各种信息，比如娱乐信息、交通状况信息、事故警告等。但是，道路上可能有自私或恶意的节点发送虚假信息。例如，恶意节点可能会伪造交通事故信息来改变其他车辆的行驶轨迹，这种虚假信息可能会影响司机的判断，危及道路安全[2]。因此，需要采取措施识别VANETs中的恶意节点和虚假信息。

传统的安全解决方案如数字签名[3]、身份认证[4]、等主要用于防范外部攻击者，无法应对经过授权的内部恶意节点。为了抵抗内部恶意节点的攻击，许多研究者提出将信任管理引入VANETs，通过信任因子收集、信任计算与决策、信任传播和信任更新等步骤，构建节点间的信任关系，从而帮助VANETs中的车辆识别恶意节点，筛选可信消息，选择可信的节点进行协作。

现有的VANETs信任管理方案主要分为三类：基于实体的信任管理方案[5-6]、基于数据的信任管理方案[7-8]和混合信任管理方案[9-10]。基于实体的信任管理方案通常以车辆之间的交互记录为信任因子，结合直接信任和推荐信任[11]计算每个车辆节点的信任值，这种方案只能识别恶意节点，并不能识别虚假消息。基于数据的信任管理方案通常利用地理位置、信号接收强度等因素来评估车辆节点收到的来自于多个信息源的数据的可信度。该方案的缺点是无法识别恶意车辆，导致恶意车辆可以在网络中一直存在，持续进行攻击。混合信任管理方案对车辆节点和数据都进行信任评估，同时具有二者的优点，但信任评估过程较为复杂，系统开销较大。但车辆节点本身具有足够可靠的存储和计算能力，可以通过采用分布式方案、限制信任评估对象的范围等方式来减少开销。此外，由于利用RSU或TA进行集中式信任管理，一旦中央服务器运行异常或受攻击，整个系统将会无法正常工作。并且，由于VANETs中消息时效性要求高，网络拓扑动态变化，集中式处理可能难以满足处理需求，分布式的信任管理方案显然更适合VANETs。

针对上述情况，本文提出了一种分布式的混合信任管理方案HTMS-V（hybrid trust management scheme for VANETs），通过对VANETs中的车辆节点和传播的数据进行信任评估，建立车辆之间的信任关系，并进行信任决策，实现VANETs中的恶意节点和虚假消息识别。本文主要贡献如下：

（1）提出了一种称为HTMS-V的VANETs信任管理方案，可以在多种攻击场景下有效识别VANETs中的恶意节点和虚假信息。

（2）提出了一种车辆节点的信任评估方法，基于VANETs的特性对主观逻辑信任模型进行了改进，结合直接信任和间接信任实现车辆节点信任评估。

（3）提出了一种基于车辆节点信任和节点间距离的消息信任评估模型。

（4）基于车辆网络仿真平台Veins验证了方案有效性，实验表明HTMS-V方案能在各种攻击场景中有效识别网络中的虚假消息和恶意节点。

1　相关工作

Jøsang[12]于2001年提出了主观逻辑，主观逻辑是一种关于真实世界主观信任操作的逻辑，用可信度评价来对主观信任进行相关描述。通过将肯定事件数、否定事件数带入Beta分布函数来进行事件可信程度的计算，最后完成信任度量工作。此后，主观逻辑信任模型被广泛地应用于各个领域的信任评估，其中也包括VANETs。

Cheng等人[13]提出了一种基于主观逻辑的信任模型来研究车辆之间的信任，并提出了一种分布式的车辆社交网络中信任评估的整体解决方案。该文假设在道路上存在车辆社交网络，其中车辆之间交换的数据是存在社会联系的，它利用车辆社交网络内的信任传播和融合来评估单个车辆的可信度。但是该文仅评估了节点间信任，没有进行消息信任评估且没有考虑到车辆的高速移动性，且为积极事件和消极事件采用相同的权重，难以识别车辆短暂的恶意行为。

Sohail等人[11]提出了一种基于主观逻辑的信任模型，旨在研究VANETs中的多跳通信环境中信任建立的问题，并在模拟实验中将信任模型应用于扩展

自组织网络按需距离矢量(ad hoc on-demand distance vector,AODV)路由协议。但是该方案只能在车辆间建立信任关系用于路由选择,不能识别网络中的虚假消息。

Kang等人[14]提出了一种基于主观逻辑计算声誉的数据共享方案,以确保车辆之间高质量的数据共享。该方案考虑了交互频率、事件及时性和轨迹相似性来计算车辆的声誉,但是没有考虑网络中可能存在的共谋攻击。

VANETs中的混合信任管理方案由于结合了基于实体的信任管理方案和基于数据的信任管理方案的优点,能识别网络中的恶意节点和虚假信息,正在被广泛研究。

Li等人[9]提出一种抗攻击信任管理方案(attack-resistant trust management scheme,ART),该方案能够检测和应对恶意攻击,并评估VANETs中传播的数据和移动节点的可信度。该方案首先收集来自多个车辆的消息数据,采用D-S证据理论来评估消息的可信度,随后基于功能信任因子和推荐信任因子,采用协同过滤算法来计算节点的可信度,但该模型在车辆较少或数据稀疏的场合下模型的评估结果准确度较差。

Soleymani等人[10]提出了一种基于经验和合理性的模糊信任模型,该模型利用消息的时间戳、发送方真实性和直接交互经验等相关因子执行一系列安全检查以确保从授权车辆接收到消息的正确性。同时,借助雾节点评估事件位置准确度来帮助检测不可信的或恶意的车辆节点。该模型仅考虑了直接信任,没有考虑间接信任,在两个节点之间缺乏交互的情况下难以进行准确的信任评估。

Ahmed等人[15]结合现有的信任管理机制,提出了一种新颖的组合信任管理框架。在此框架中,节点从收到的消息中迭代地了解环境,推荐信任模块通过使用来自同一发送者的连续消息中接收到的信息的相似性和一致性来确定推荐的可信度;节点信任模块根据接收者自己的经验以及邻居的推荐来更新节点的信任值;事件信任模块在决策逻辑中确定报告的事件是否实际发生。该框架允许节点识别和过滤来自恶意节点的推荐,并辨别真实事件。该框架接收的推荐为二元意见(0表示节点不可信,1表示节点可信),形成的推荐信任不够准确。

Oubabas等人[16]提出了一种基于信任的聚类算法,该算法根据集群成员之间移动性的相似性为节点分配角色,基于稳定性和信任因素来选择可信赖的簇头。为了确保车辆间良好的协作和可靠的数据共享,本方案在信任管理中,基于车辆的合作度和其广播信息的合法性来评估车辆节点的信任。同时,提出了一种具有严重性参数的自适应信任函数来评估网络中的数据信任。Hasrouny等人[17]提出了基于组的混合信任模型和不当行为检测系统,车辆之间基于车辆行为进行信任评估,在同一区域内选择信任值最高的节点作为组长动态管理组内成员,基于不当行为检测系统检测可能存在的恶意车辆。以上两个方案都不够稳定,由于车辆的移动性,可能需要频繁地进行重新分组和簇头选择,影响方案后续的信任评估。

Fan等人[18]提出了一种集成的安全方案,以帮助VANETs中的节点识别网络中的合法消息以做出正确的决策。该方案首先构建信任模型来量化节点声誉,通过观察节点的通信行为来衡量节点的直接声誉,并综合来自节点的邻居和路边单元报告的信息来确定其间接声誉。并且基于上述信任模型,进一步设计了一种用于识别合法消息的属性加权*K*-means算法和一种用于VANETs中消息传递的路由方法。但是该方案的信任评估需要RSU参与,时间开销较大,信任更新不够快速。

Zhang等人[19]提出了一个基于区块链的信任管理系统,基于贝叶斯推理判断消息可信度,基于加权聚合进行车辆信任评估,采用工作量证明(proof of work,PoW)和权益证明(proof of stake,PoS)相结合的共识机制,基于区块链进行信任数据的存储和更新。Li等人[20]同样提出了一种基于区块链的信任管理方案,车辆之间基于时间、位置、历史信任评估彼此可信度,还设计了一种共识机制,某个区域内的所有RSU共同维护一个联盟链,部分RSU对区块进行验证,所有RSU根据规则同步信任数据。但是基于区块链的信任管理方案存在区块链更新速度太慢,难以满足VANETs中消息时效性要求的问题,以及存在RSU上传虚假数据的可能性。

综上所述,现有的VANETs信任管理方案中依赖于RSU或车辆簇头的方案存在不能适应网络动态变化、信任更新不够快速的问题并且很少考虑RSU本身是恶意节点的问题;完全分布式的方案则存在信任评估不准确、没有考虑到可能存在的共谋攻击、信任评估因子考虑不全等问题。本文旨在研究一种更全面的信任管理方案,以完全分布式的信任管理方

案适应网络动态变化，全面考虑直接信任和间接信任设计信任评估方案提供准确的信任评估，能帮助车辆在多种攻击场景下识别网络中的恶意节点和虚假消息以进行正确的决策。

2　问题描述

2.1　系统模型

VANETs主要由车辆节点、RSU和TA组成，但是由于在信任管理中依赖RSU或TA的支持会增加网络开销从而影响系统的动态运行，本文的信任管理方案不依赖它们，信任数据的计算和管理由车辆节点单独处理。在本文的方案中，每个车辆节点都配备了一个车载单元（on board unit，OBU），能够与其他OBU进行通信，并可处理和存储信任数据。车辆节点定期发送信标消息，与其他节点交换交通和道路信息。每个车辆节点上都部署了信任评估模块和信任决策模块，并且维护各自的邻居节点信息表用于记录邻居节点信息和交互历史。

2.2　对手模型

本文假设攻击者是VANETs内部的车辆节点，它能够窃听、干扰其通讯范围内任意节点之间的无线通信。对手的主要目标可能包括伪造或修改数据、提交虚假信任推荐诋毁普通节点等。具体来说，包括以下攻击能力：

（1）虚假消息注入攻击：恶意节点伪造虚假信息注入网络，如伪造交通事故信息、传播虚假路况信息等。但在信任评估过程中，它们不会提供虚假的信任推荐。

（2）开关攻击：有时恶意节点会改变它们的行为模式，使它们更难被检测到。例如，它们通过一段时间的良好行为提升自己的信任值，然后展开攻击。此外，恶意节点也会对不同的节点表现出不同的行为，从而导致不同节点之间对同一节点的信任意见不一致。由于这类节点的攻击行为并不持续，通常很难识别它们。

（3）共谋攻击：恶意节点除了进行虚假消息注入攻击外，还传播虚假的信任推荐，试图降低普通节点信任值，增加恶意节点信任值。其目的在于破坏准确的信任评估，使普通节点难以成功识别恶意节点。

3　HTMS-V方案设计

本章提出了一种基于主观逻辑的混合信任管理方案HTMS-V，其概述如图1所示。

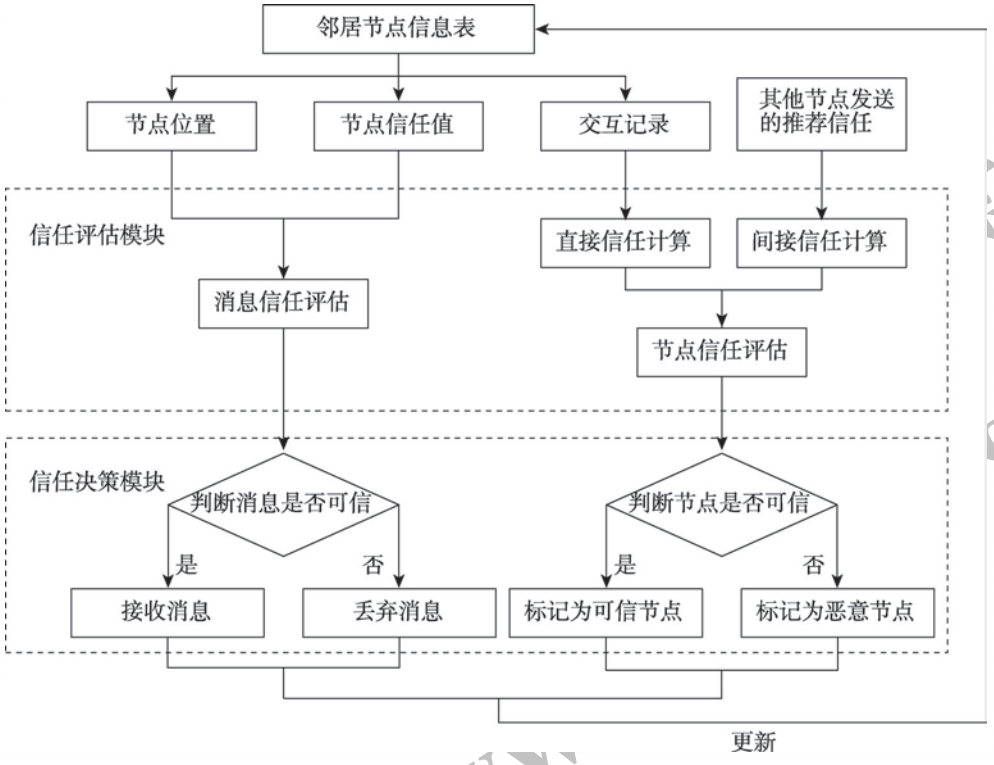

图1　HTMS-V概览

Fig.1　Overview of HTMS-V scheme

在HTMS-V中,车辆节点首先基于邻居节点信息表中的交互记录计算得到直接信任值,通过接收其他车辆发送的推荐信任计算间接信任值,随后结合直接信任值和间接信任值得到对每个邻居节点的信任值。如果信任值低于阈值将被判定为恶意节点。每当车辆节点收到网络中的广播消息,由信任评估模块结合节点信任值和节点位置,计算广播消息的信任值并进行信任决策,并更新其邻居节点信息表。本文方案无需RSU和TA参与,车辆节点根据自身存储的信息和周围车辆的信任推荐进行信任评估,能适应网络动态变化,随时对遇到的新节点和收到的新消息进行信任评估。

3.1 主观逻辑信任模型

HTMS-V基于主观逻辑[12]进行车辆节点的信任评估,主观逻辑的概念中存在“证据空间”和“观察空间”这两个概念。“证据空间”由肯定与否定事件组成,为信任模型提供信任评价的信任证据,而“观念空间”就是信任度,反映了事物的信任程度。实体A对实体B的信任度w_B^A可以由三元组(b_B^A,d_B^A,u_B^A)表示,b_B^A、d_B^A、u_B^A分别表示实体A对B的信任程度、不信任程度和不确定程度。

为了准确反映信任状态,主观逻辑信任模型给出了“证据空间”到“观念空间”的映射关系:

$$\begin{cases} b_B^A = \dfrac{S}{S+F+1} \\ d_B^A = \dfrac{F}{S+F+1} \\ u_B^A = \dfrac{1}{S+F+1} \end{cases} \tag{1}$$

其中,S为肯定事件数,F为否定事件数。

在网络中,不同节点对同一节点存在各自的信任评价,通常需要组合多个来源的信任评价来对一个节点进行相对准确的信任评估。在主观逻辑信任模型中,定义了信任组合符号$\oplus$,设实体A和实体B对实体C的信任评价分别为$w_C^A=(b_C^A,d_C^A,u_C^A)$、$w_C^B=(b_C^B,d_C^B,u_C^B)$,信任组合计算公式如下:

$$\begin{cases} w_C^{AB} = w_C^A \oplus w_C^B \\ b_C^{AB} = \dfrac{b_C^A \times u_C^B + b_C^B \times u_C^A}{k} \\ d_C^{AB} = \dfrac{d_C^A \times u_C^B + d_C^B \times u_C^A}{k} \\ u_C^{AB} = \dfrac{u_C^A \times u_C^B}{k} \end{cases} \tag{2}$$

其中,

$$k = u_C^A + u_C^B - u_C^A \times u_C^B \tag{3}$$

本方案在此基础上,考虑到车载自组织网络的特性做出了一些改进来进行车辆节点的信任评估。

3.2 车辆节点信任评估

3.2.1 直接信任

在车载自组织网络中,由于车辆的高移动性,车辆间的信任关系通常是不长久的,主观逻辑信任模型可能很难识别短暂经过的恶意车辆,因此需要在其基础上加入对失败交互的惩罚因子和用于调整不确定性的参数。

基于此,本文方案直接信任值DT_B^A的计算公式如下:

$$\begin{cases} b_B^A = \dfrac{S}{S+\beta F+m} \\ d_B^A = \dfrac{S}{S+\beta F+m} \\ u_B^A = \dfrac{m}{S+\beta F+m} \end{cases} \tag{4}$$

$$DT_B^A = b_B^A + \alpha_1 u_B^A \tag{5}$$

其中,S为交互成功次数,F为交互失败次数;参数β是对失败交互的惩罚因子,β越大,失败交互引起的信任值下降越快;参数m是用于调整不确定性的参数,m越大,不确定性下降越慢。

对于初次相遇的车辆C和D,其交互成功次数和交互失败次数均为0,C对D的直接信任计算如下:

$$\begin{cases} b_D^C = \dfrac{S}{S+\beta F+m} = 0 \\ d_D^C = \dfrac{S}{S+\beta F+m} = 0 \\ u_D^C = \dfrac{m}{S+\beta F+m} = 1 \end{cases}$$

$$DT_C^C = b_C^C + \alpha_1 u_D^C = \alpha_1$$

即车辆之间的初始信任为设定的参数α_1。

3.2.2 间接信任

节点间接信任值由组合第三方对节点的推荐信任进行计算得到,考虑到车载自组织网络中对消息实时性的要求,本文方案只接收周围一跳邻居的推荐信任,按照主观逻辑信任模型中的信任组合计算方式计算。如果节点A收到节点$\{C,D,\cdots,M\}$对节点B的推荐信任$\{w_B^C,w_B^D,\cdots,w_B^M\}$,则节点$A$对节点$B$的间接信任值$RT_B^A$的计算公式如下:

$$w_B^{CD\cdots M} = (b_B^{CD\cdots M}, d_B^{CD\cdots M}, u_B^{CD\cdots M}) = w_B^C \oplus w_B^D \oplus \cdots \oplus w_B^M \tag{6}$$

$$RT_B^A = b_B^{CD\cdots M} + \alpha_2 u_B^{CD\cdots M} \tag{7}$$

考虑到网络中可能存在错误的信任推荐和恶意车辆发送的虚假信任推荐,本文方案设置了推荐信任接收阈值$Threshold_R$,当节点A收到节点C对B的推荐信任$w_B^C=(b_B^C,d_B^C,u_B^C)$,但满足$|T_B^A-(b_B^C+\alpha_1 u_B^C)|>Threshold_R$

时，节点A将认为节点C的推荐信任不可信，拒绝接收。

3.2.3　综合信任

最后，结合直接信任值和间接信任值进行综合信任值的计算，节点A对节点B的综合信任值T_B^A计算公式如下：

$$T_B^A = w_d DT_B^A + w_r RT_B^A \tag{8}$$

其中，w_d和w_r分别为直接信任值和间接信任值的权重。间接信任的引入是由于在实际中，可能缺乏足够的直接交互经验来做出信任评价，因此需要借助第三方的推荐，但是第三方不一定完全可靠。随着直接交互次数的增多，节点应更依赖于直接信任，直接信任值的权重应该随着两个节点之间交互次数的增加而增大。本文方案采用Parhizkar等人[21]提出的指数函数计算直接信任值和间接信任值的权重，w_d和w_r的计算公式如下：

$$w_r = \mathrm{e}^{-\lambda n} \tag{9}$$

$$w_d = 1 - w_r \tag{10}$$

其中，n为节点A与节点B的交互次数，参数λ为交互次数的系数。设置信任阈值$Threshold_T$，当$T_B^A < Threshold_T$时，节点A将认为节点B是恶意节点。

3.3　VANETs消息可信性评估

消息的可信性应该与节点的信任值和节点间距离相关。通常来说，由于地理位置上越相近的车辆遇到的道路状况、交通状况越相似，车辆节点之间的距离越小，对其发出的消息的信任程度应该越高。并且一个节点的信任值越高，它发送的消息就越可信。

在行驶过程中，车辆节点i可能收到关于事件e的不同消息$\{e_1,e_2,\cdots,e_n\}$，此时，车辆节点将对收到的关于事件e的每种消息进行可信性评估。假设车辆节点i收到了来自节点$\{a_1,a_2,\cdots,a_m\}$发送的消息e_j，车辆节点i对消息e_j的可信性评估公式如下：

$$T_{e_j} = \frac{T_{a_1}^i}{d_1} + \frac{T_{a_2}^i}{d_2} + \cdots + \frac{T_{a_m}^i}{d_m} \tag{11}$$

其中，$\{T_{a_1}^i, T_{a_2}^i, \cdots, T_{a_m}^i\}$分别为车辆节点$i$对节点$\{a_1, a_2, \cdots, a_m\}$的综合信任值，$\{d_1,d_2,\cdots,d_m\}$分别为节点$\{a_1,a_2,\cdots,a_m\}$到车辆节点$i$的距离。

关于事件e的不同消息$\{e_1,e_2,\cdots,e_n\}$的消息可行性评估完成后，车辆节点根据信任值进行信任决策。

综上所述，本文方案考虑到了车载自组织网络通信的实时性要求，且能适应网络动态变化，基于主观逻辑信任模型设计了车辆节点的信任评估方案。在车辆节点的信任评估中，基于交互记录进行直接信任的评估，综合推荐信任得到间接信任值，基于交互次数计算直接信任与间接信任的权重；消息可信性则基于节点的信任值和节点之间的距离进行评估，通过准确的信任评估来建立车辆节点之间的信任关系，识别网络中的虚假消息。

4　仿真实验及结果分析

4.1　对比方案设置

由于HTMS-V方案中节点信任评估方案是基于主观逻辑信任模型改进得到的，消息可信性评估方案是基于距离的加权投票进行改进得到的，将对比实验的Baseline方案设置为了基于主观逻辑的节点信任评估和基于距离的加权投票的消息可信性评估。具体评估方式如下：

节点A对B的直接信任值DT_B^A计算公式如下：

$$\begin{cases} b_B^A = \dfrac{S}{S+F+1} \\ d_B^A = \dfrac{F}{S+F+1} \\ u_B^A = \dfrac{1}{S+F+1} \end{cases} \tag{12}$$

$$DT_B^A = b_B^A + \alpha_3 u_B^A \tag{13}$$

如果节点A还收到节点$\{C,D,\cdots,M\}$对节点B的推荐信任$\{w_B^C, w_B^D, \cdots, w_B^M\}$，则节点$A$对节点$B$的综合信任值计算公式如下：

$$w_B^{ACD\cdots M} = (b_B^{ACD\cdots M}, d_B^{ACD\cdots M}, u_B^{ACD\cdots M}) = w_B^A \oplus w_B^C \oplus w_B^D \oplus \cdots \oplus w_B^M \tag{14}$$

$$T_B^A = b_B^{ACD\cdots M} + \alpha_4 u_B^{ACD\cdots M} \tag{15}$$

假设车辆节点i收到了来自节点$\{a_1,a_2,\cdots,a_m\}$发送的消息e_j，车辆节点i对消息e_j的可信性评估公式如下：

$$T_{e_j} = \frac{min_d}{d_1} + \frac{min_d}{d_2} + \cdots + \frac{min_d}{d_m} \tag{16}$$

其中，min_d为车辆节点i与最近的一个节点之间的距离，$\{d_1,d_2,\cdots,d_m\}$分别为节点$\{a_1,a_2,\cdots,a_m\}$到车辆节点i的距离。

4.2　实验设置

选用Veins[22]作为仿真实验的平台，它是一个用于运行车辆网络模拟的开源框架，由基于事件的网络模拟器OMNet++[23]和道路交通模拟器SUMO[24]构成。

本文选取了一段真实世界中的一组普通城市道

路及周边建筑，基于SUMO生成了实验地图来模拟常见的市区交通场景，道路限速55 km/h。

网络中的每个车辆节点周期性广播信标消息，信标消息内容包括车辆id、车辆基本行驶状况、对邻居节点的推荐信任表、道路状况。车辆节点接收到某个邻居广播的信标消息时，将其内容写入邻居节点信息表。车辆节点通过信任计算，周期性地对道路状况信息进行判断，然后车辆节点对消息进行反馈，计算邻居节点信任并更新邻居节点信息表。

最后，采用消息判断准确率、恶意节点判断准确率、节点误报率作为信任管理方案的评估标准，计算公式如下：

$$\text{消息判断准确率}=\frac{\text{正确判断的消息数}}{\text{判断的消息总数}} \tag{17}$$

$$\text{恶意节点判断准确率}=\frac{\text{正确识别的恶意节点数}}{\text{恶意节点总数}} \tag{18}$$

$$\text{节点误报率}=\frac{\text{被误报为恶意节点的普通节点数}}{\text{普通节点总数}} \tag{19}$$

为了评估本文方案在不同攻击下的性能，设置了四种攻击场景分别进行实验。在实验中，利用SUMO生成了20个随机车流文件，每种攻击场景都使用这20个随机车流文件进行20次实验，取平均结果作为实验最终结果，实验参数如表1所示。

表1 实验参数

Table 1 Experimental parameters

参数	值
仿真区域/km²	3×3
仿真时间/s	800
节点个数	200
最大车速/(km/h)	55
信标消息周期/s	2
信任更新周期/s	10
β、m	2,2
α_1、α_2	0.5,0.5
α_3、α_4	0.5,0.5
λ	0.1
$Threshold_R$	0.4
$Threshold_T$	0.5

4.3 实验与分析

4.3.1 抗虚假消息注入攻击能力分析

假设恶意节点持续发送虚假消息，在恶意节点率为10%、20%、30%、40%的情况下分别进行了实验，实验结果如图2所示。

在恶意节点率为10%~30%的情况下，HTMS-V方案的消息判断准确率和恶意节点判断准确率高于92%，误报率低于6%，恶意节点率上升到40%时方案性能有较大幅度下降，但是现实中很难遇到恶意节点率如此高的情况。相较于对比方案，在这种攻击场景下二者性能相差不大，HTMS-V方案的消息判断准确率和恶意节点判断准确率略高于对比方案，而误报率也略高。

4.3.2 抗开关攻击能力分析

在开关攻击中，恶意节点虚假消息与真实消息交替发送，在恶意节点率为10%、20%、30%、40%的情况下分别进行了实验，实验结果如图3所示。

在此攻击场景下，HTMS-V方案的消息判断准确率保持在98%以上，恶意节点判断准确率保持在97%以上，误报率保持在8%以下，这表明HTMS-V方案能有效抵抗开关攻击。相较于对比方案，HTMS-V方案的性能明显更好，恶意节点判断准确率大幅高于对比方案。主要是因为在实验中，HTMS-V方案的节点信任计算将失败交互的惩罚因子设置为2，使得节点的恶意行为较大幅度引起信任值下降，而良好行为引起的信任值上升则较慢。但这同时也导致了误

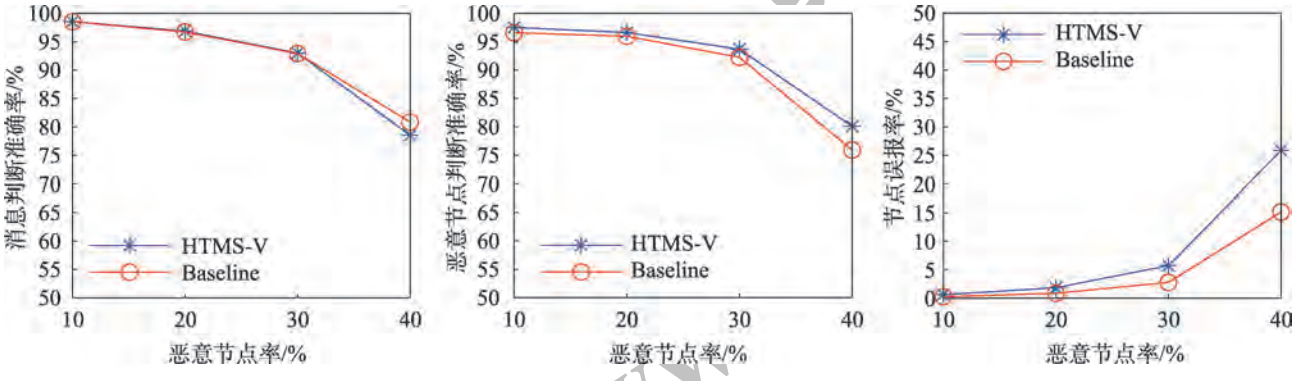

图2 虚假消息注入攻击检测性能对比

Fig.2 Performance comparison of false message injection attack detection

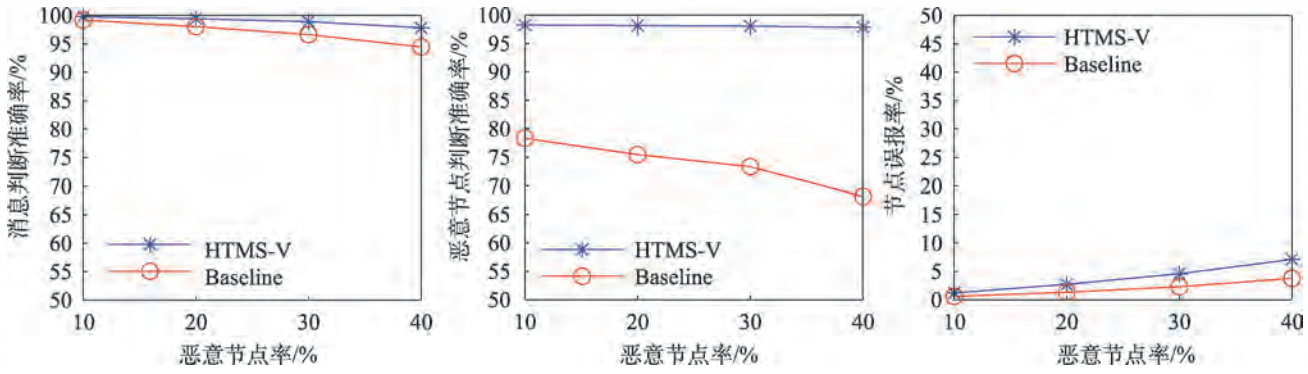

图3　开关攻击检测性能对比

Fig.3　Performance comparison of on-off attack detection

报率的升高，实验结果显示HTMS-V方案的误报率略高于对比方案。但从整体来看，误报率的小幅升高换取大幅恶意节点识别准确率的提升是完全值得的。

4.3.3　抗共谋攻击能力分析

在共谋攻击中，恶意节点持续发送虚假消息并且发送虚假的推荐信任，对其他恶意节点的推荐信任为 b=100/102，u=2/102；对普通节点的推荐信任为 b=0，u=2/102（即恶意节点假设和其他恶意节点已经有了100次成功交互，和普通节点有100次失败交互）。在恶意节点率为10%、20%、30%、40%的情况下分别进行了实验，实验结果如图4所示。

在恶意节点率10%~30%的情况下HTMS-V方案的消息判断准确率和恶意节点判断准确率高于92%，误报率低于8%，这表明HTMS-V方案能有效抵抗共谋攻击。虽然当恶意节点率上升到40%时方案性能有较大幅度下降，但是现实中很难遇到恶意节点率如此高的情况。相较于对比方案，HTMS-V方案的性能明显更好，消息判断准确率和恶意节点判断准确率都明显高于对比方案，误报率也低于对比方案。这首先是因为HTMS-V方案设置了推荐信任接收阈值，拒绝了与节点存储的信任值相差较大的推荐信任，并且由于在HTMS-V模型中，间接信任的权重是随交互次数的增大而减小的指数函数，使得在进行了一定交互后普通节点即使接收了虚假信任推荐，其造成的信任值变化也较小。

4.3.4　抗混合攻击能力分析

在真实的交通场景中，可能发生的攻击类型不止一种，本小节混合了上述三种恶意节点，在进行虚假消息注入攻击、开关攻击、共谋攻击的恶意节点率各为3%、5%、7%、9%，即总恶意节点率分别为9%、15%、21%、27%的情况下进行了实验，实验结果如图5所示。

在此攻击场景下，HTMS-V方案的消息判断准确率保持在95%以上，恶意节点判断准确率保持在96%以上，误报率保持在4%以下，这表明HTMS-V方案能有效抵抗混合攻击。相较于对比方案，HTMS-V的性能明显更好，各项指标均明显优于对比方案。

与近年来文献提出的分布式混合信任管理方案[10,15-17]相比，在恶意节点率低于30%时各方案性能

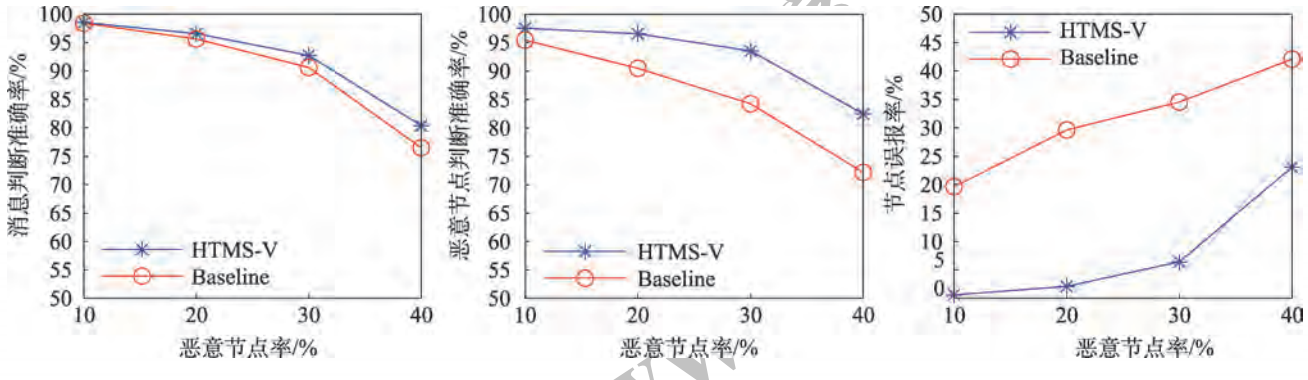

图4　共谋攻击检测性能对比

Fig.4　Performance comparison of bad mouth attack detection

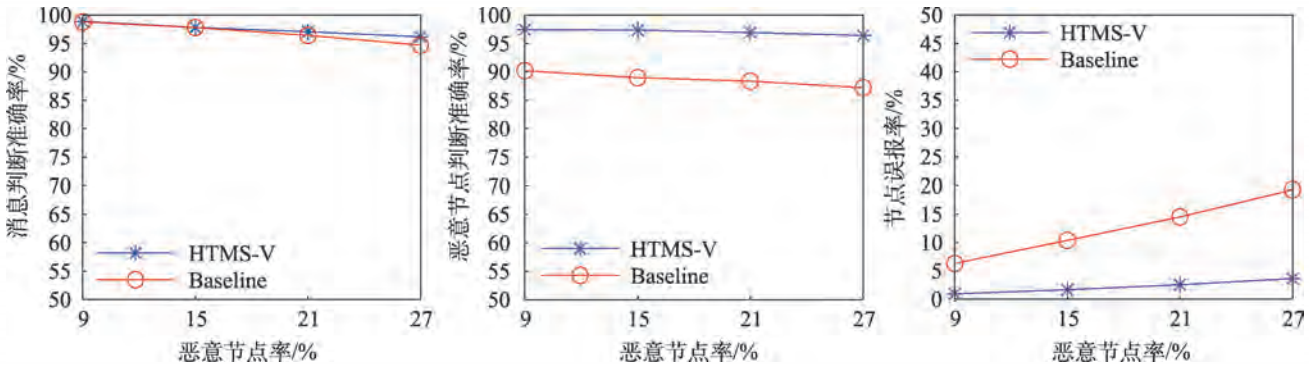

图5 混合攻击检测性能对比

Fig.5 Performance comparison of hybrid attack detection

相差不大,均能高效识别网络中的恶意节点和虚假消息。其中,Oubabas等人[16]提出的方案由于选择簇头需要额外的通信开销,并且更换簇头可能导致方案性能不稳定。当恶意节点率较高时,Ahmed等人提出的方案[15]效果最优,在80%的恶意节点情况下仍能有效识别网络中的恶意节点和虚假消息,但这现实意义不大,因为现实中很难遇到如此密集的恶意车辆。本文方案的优势在于除了能够检测网络中的恶意节点和虚假消息,还能有效抵抗多种攻击。由于在信任评估过程中加入了不确定性参数和对失败交互的惩罚因子,方案可以有效抵御开关攻击;由于方案中基于交互次数的直接信任/间接信任的权重计算方式以及推荐信任接收阈值的设置,方案可以有效抵抗共谋攻击。并且由于信任管理过程不依赖于RSU、TA或车辆簇头,车辆可以随时对新加入的车辆节点和新接收到的消息进行信任评估,因此能适应网络动态变化,能够满足车载自组织网络对消息实时性的要求。

5 结束语

本文面向VANETs中恶意节点和虚假消息检测提出了一种混合信任管理方案,构建了基于主观逻辑信任模型的节点信任评估模型和基于节点信任和距离的消息信任评估模型。实验结果表明,在多种攻击场景下,HTMS-V方案均能有效识别网络中的恶意节点和虚假消息。且较之于主观逻辑模型和基于距离的加权投票法构成的基线方案,HTMS-V有更好表现,在开关攻击场景下,消息判断准确率和恶意节点判断准确率明显优于基线方案,在共谋攻击和混合攻击场景下,消息判断准确率、恶意节点判断准确率和误报率都明显优于基线方案。

参考文献:

[1] CUNHA F, VILLAS L, BOUKERCHE A, et al. Data communication in VANETs: protocols, applications and challenges[J]. Ad Hoc Networks, 2016, 44: 90-103.

[2] HUSSAIN R, LEE J, ZEADALLY S. Trust in VANET: a survey of current solutions and future research opportunities [J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(5): 2553-2571.

[3] ZHANG L, WU Q, DOMINGO-FERRER J, et al. Distributed aggregate privacy-preserving authentication in VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(3): 516-526.

[4] LUO M, ZHOU Y. An efficient conditional privacy-preserving authentication protocol based on generalized ring signcryption for VANETs[J]. IEEE Transactions on Vehicular Technology, 2022, 71(9): 10001-10015.

[5] GÓMEZ MÁRMOL F, MARTÍNEZ PÉREZ G. TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks[J]. Journal of Network and Computer Applications, 2012, 35(3): 934-941.

[6] FABI A K, THAMPI S M. A trust management framework using forest fire model to propagate emergency messages in the Internet of vehicles (IoV) [J]. Vehicular Communications, 2022, 33: 100404.

[7] GURUNG S, LIN D, SQUICCIARINI A, et al. Information-oriented trustworthiness evaluation in vehicular ad-hoc networks[C]//Proceedings of the 7th International Conference on Network and System Security, Madrid, Jun 3-4, 2013: 94-108.

[8] SUN M, LI M, GERDES R. A data trust framework for VANETs enabling false data detection and secure vehicle tracking[C]//Proceedings of the 2017 Conference on Communications and Network Security, Las Vegas, Oct 9-11, 2017: 1-9.

[9] LI W, SONG H. ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(4): 960-969.

[10] SOLEYMANI S A, ABDULLAH A H, ZAREEI M, et al. A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing[J]. IEEE Access, 2017, 5: 15619-15629.

[11] SOHAIL M, WANG L, JIANG S, et al. Multi-hop interpersonal trust assessment in vehicular ad-hoc networks using three-valued subjective logic[J]. IET Information Security, 2019, 13(3): 223-230.

[12] JØSANG A. A logic for uncertain probabilities[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001, 9(3): 279-311.

[13] CHENG T, LIU G, YANG Q, et al. Trust assessment in vehicular social network based on three-valued subjective logic [J]. IEEE Transactions on Multimedia, 2019, 21(3): 652-663.

[14] KANG J, YU R, HUANG X, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks[J]. IEEE Internet of Things Journal, 2019, 6(3): 4660-4670.

[15] AHMED S, AL-RUBEAAI S, TEPE K. Novel trust framework for vehicular networks[J]. IEEE Transactions on Vehicular Technology, 2017, 66(10): 9498-9511.

[16] OUBABAS S, AOUDJIT R, RODRIGUES J J P C, et al. Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme[J]. Vehicular Communications, 2018, 13: 128-138.

[17] HASROUNY H, SAMHAT A E, BASSIL C, et al. Trust model for secure group leader-based communications in VANET[J]. Wireless Networks, 2018, 25(8): 4639-4661.

[18] FAN N, WU C Q. On trust models for communication security in vehicular ad-hoc networks[J]. Ad Hoc Networks, 2019, 90: 101740.

[19] ZHANG H, LIU J, ZHAO H, et al. Blockchain-based trust management for internet of vehicles[J]. IEEE Transactions on Emerging Topics in Computing, 2021, 9(3): 1397-1409.

[20] LI M, ZHAO G, LAI R. A scalable blockchain-based trust management strategy for vehicular networks[C]//Proceedings of the 17th International Conference on Wireless Algorithms, Systems, and Applications, Dalian, Nov 24-26, 2022: 285-295.

[21] PARHIZKAR E, NIKRAVAN M H, HOLTE R C, et al. Combining direct trust and indirect trust in multi-agent systems[C]//Proceedings of the 29th International Joint Conference on Artificial Intelligence, Yokohama, Jul 2020: 311-317.

[22] SOMMER C, GERMAN R, DRESSLER F. Bidirectionally coupled network and road traffic simulation for improved IVC analysis[J]. IEEE Transactions on Mobile Computing, 2011, 10(1): 3-15.

[23] VARGA A, HORNIG R. An overview of the OMNeT++ simulation environment[C]//Proceedings of the 1st International ICST Conference on Simulation Tools and Techniques for Communications, Networks and Systems, Marseille, Mar 3-7, 2008: 1-10.

[24] BEHRISCH M, BIEKER L, ERDMANN J, et al. SUMO—simulation of urban mobility: an overview[C]//Proceedings of the 3rd International Conference on Advances in System Simulation, Barcelona, Oct 23-28, 2011: 55-60.

项丹(1997—),女,浙江宁波人,硕士研究生,主要研究方向为车载自组织网络安全。

XIANG Dan, born in 1997, M.S. candidate. Her research interest is security of VANETs.

陈泽茂(1975—),男,福建福清人,博士,教授,博士生导师,主要研究方向为系统安全与可信计算。

CHEN Zemao, born in 1975, Ph.D., professor, Ph.D. supervisor. His research interests include system security and trusted computing.