文章编号：2095-2163(2021)11-0174-06 中图分类号：TP391 文献标志码：A

基于动态聚类的 VANET 信任模型的设计

齐健翔[1]，岳克强[2]
（1 新乡学院 计算机与信息工程学院，河南 新乡 453003；2 杭州电子科技大学 电子信息学院，杭州 310018）

摘 要： VANET 受限于车辆的高速移动性，网络拓扑的动态性及无线信道的开放性，极易遭受来自网络内部的差评攻击和选票攻击。为了保障 VANET 通信安全，本文提出了一种基于动态聚类的信任模型，通过去除推荐信任中与主观信任偏离度较大的数据，最大化包含评估节点邻域内的有效信息，从而减少恶意攻击对信任计算造成的影响。实验表明，该模型具有较强的抗攻击性和鲁棒性。随着 VANET 中攻击节点所占比例的增加，网络能够保持较高的吞吐量和较低的丢包率，模型的计算结果能够保持较高的准确性。

关键词： 信任模型；动态聚类；差评攻击；选票攻击

Design of VANET trust model based on dynamic clustering

QI Jianxiang[1], YUE Keqiang[2]
(1 School of Computer and Information Engineering, Xinxiang University, Xinxiang Henan 453003, China;
2 School of Electronic Information, Hangzhou Dianzi University, Hangzhou 310018, China)

【Abstract】 VANET is limited by the high-speed mobility of vehicles, the dynamics of network topology and the openness of wireless channels, and it is extremely vulnerable to bad-mouth attack and ballot attack from the internal of network. In order to protect the communication security of VANET, propose a trust management model based on dynamic clustering. The effective information in the neighborhood of the evaluation node is maximized by removing the data which has a large deviation with subjective judgement in the recommendation, and the impact of malicious attacks on the trust calculation is reduced. According to the experiments, it shows that the model has strong anti-attack and robustness. As the proportion of attacking nodes in VANET increases, the network can maintain a higher throughput and a lower packet loss rate, and the calculation results of the model can maintain higher accuracy.

【Key words】 trust model; dynamic clustering; bad-mouth attack; ballot attack

0 引 言

车载自组织网络(Vehicular Ad-hoc Network, VANET)是指行驶道路上的车辆之间在没有其它既定基础设施的情况下，相互通信而形成的自组织无线网络，是智能交通系统(ITS)的核心组成部分[1-2]。由于 VANET 的分布特性，车辆之间必须相互协作，以支持网络的正常运行。车辆的高速移动性决定了 VANET 的拓扑结构具有一定的复杂性和易变性，这意味着车辆将会始终处于一个“陌生”的网络环境中，车辆之间无法建立长期稳定的合作关系。此外，无线通信的广播性及通信标准的开放性也会导致车辆之间的通信过程极易遭受恶意攻击和破坏，通信内容可能会被伪造和篡改[3-4]。保护 VANET 通信安全，使其免受广泛攻击是网络安全领域的一项重要挑战，VANET 中常见的攻击行为主要包括：黑洞攻击、开关攻击、差评攻击及选票攻击等[5]。VANET 通信安全问题涉及到车辆行驶安全和交通管理效率，甚至在一些紧急情况下可能会危及乘客及行人的生命安全，成为制约车联网部署和实施的关键因素，是当前车联网应用研究中最受关注的问题之一[6-7]。

1 国内外研究现状

现有的网络通信安全研究主要分为密码学技术和非密码学技术两大类[8]。传统的基于密码学的方法较为成熟，适用于处理外部人员发动的恶意攻击。而对于内部攻击者而言，由于其本身已经拥有合法身份，密码学技术在处理此类攻击方面收效甚微。影响 VANET 通信安全的恶意攻击行为通常来

基金项目： 浙江省重点研发计划项目(2019C01070)。

作者简介： 齐健翔(1983-)，男，硕士，助教，主要研究方向：物联网技术应用、物联网安全；岳克强(1984-)，男，博士，讲师，主要研究方向：无线自组网应用、移动计算、信息物理系统安全。

通讯作者： 齐健翔 Email：qjx1011@126.com

收稿日期： 2021-09-24

自网络内部，需要采用基于非密码学技术的方法进行处理，信任管理方法便是其中的典型代表。根据不同的理论依据和处理机制，信任管理方法可划分为多种不同类别，如图 1 所示[9]。

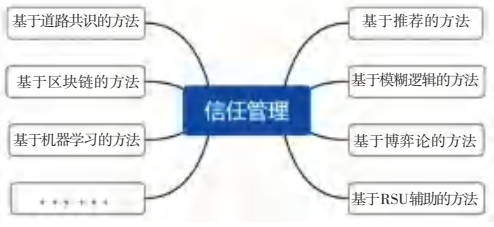

图 1　信任管理分类

Fig. 1　Classifications of trust management

目前，VANET 中信任管理的研究工作涉及到车辆之间，车辆与路侧基础设施（Road Side Unit，RSU）之间通信过程的各个方面[10]。Chen 等提出了一种基于信标（Beacon）的信任管理系统 BTM，车辆之间借助 Beacon 信息来构建网络节点间的信任关系，据此判断接收到的直接或间接事件信息是否可信，从而防止内部攻击者在网络中发送虚假信息[11]；Al Falasi 等通过对同一事件不同来源的信息内容进行相似性分析，提出了一种基于内容相似性的信任管理方案[12]；Chen 等通过结合底层网络拓扑信息，提出了一种新颖的启发式最优决策算法，无需获取当前网络中恶意攻击者的分布比例等先验知识，仅依靠部分拓扑信息就能够实现对接收信息的可信度进行有效判定，极大地提高了网络的安全性能[13]；Hasrouny 等提出一种基于群组管理的混合信任模型，根据车辆的通信范围动态建组，选择最可靠的节点负责内部管理以及与 RSU 交互[14]。通过采用集中式和分布式相结合的信任管理方案，可以有效地区分正常车辆和恶意车辆，同时有效地保障了成员节点的隐私，网络开销较低。

2　信任评估模型

在 VANET 中利用信任评估模型能够获取充足的信息来分析节点是否可信，进而判断其工作状态和类别属性。一方面可以激励那些信任度较高的节点继续保持良好的通信行为；另一方面惩罚那些信誉度较低的节点，防止其继续采取不良的通信行为。当节点的信任度下降到一个极低的水平时，强制剥夺该节点在当前网络中的合法身份，避免其恶意攻击行为造成严重后果。

VANET 中常用的信任评估模型大都是采用分布式算法，在网络中各个节点之间进行信任度的量化评估。现有的研究成果将节点信任度的评估模型大致分为 3 类，即：（1）从主观方面出发，根据评估节点与被评估对象的直接交互，计算对方的信任度，称为“主观信任”（Subject Trust，ST）；（2）从客观方面，根据网络中其他节点的推荐信息来计算被评估对象的信任度，称为“推荐信任”（Recommendation Trust，RT）；（3）综合考虑主、客观因素，混合计算被评估节点的可信度，也称为“全局信任”（Global Trust，GT）[15]。鉴于 VANET 中节点数量众多且处于高速移动状态，网络拓扑变化较大，通信环境较为复杂且不稳定，无法仅仅凭借有限的直接交互做出与真实情况相符的主观判断，需要在周围车辆的辅助下全面审视评估对象的真实可信度。因此，本文采用第三种综合计算方法来评估节点的全局信任度。

2.1　主观信任计算

主观信任是指网络中的相邻节点通过分析彼此间的交互行为从而构建的一种信任关系，这种关系有助于评估节点决定是否信任对方及其提供的数据信息。在 VANET 中，节点间通信的历史行为具有一定的统计意义，并对节点未来可能会采取的行为产生很大的影响。因此，本文利用贝叶斯统计方法来计算车辆的信任值。车辆节点的信任度通常服从 Beta 概率分布，可以利用 α 和 β 这两个参数来进行信任值的估算，α 和 β 分别为节点之间交互成功和失败的次数。Beta 分布可以由 *gamma* 函数定义，公式（1）如下：

$$f(p \mid \alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha) * \Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \quad (1)$$

本文使用 ST（Subject Trust）来表示直接信任度，节点 i 对相邻节点 j 的直接信任度设为 ST_{ij}。由公式（1）可知，当前时刻 ST_{ij} 对应 Beta 分布的期望值，即式（2）：

$$ST_{ij} = \frac{\alpha}{\alpha+\beta} \quad (2)$$

其中，α 和 β 均为大于 0 的正数且初始值为 1，这也意味着当车辆 i 和车辆 j 首次见面时由于没有历史交互信息，二者的直接信任度默认为 0.5，即：不确定的信任状态。

为了防止恶意节点通过伪装和欺骗快速提高其信任度，例如：恶意车辆发动开关攻击，在相同条件下，信任值随着良性行为次数的累计而缓慢增长，随着恶意行为如：丢包、拒绝转发数据包等次数的累计

而迅速下降,即:“做坏事”受到的惩罚远大于“做好事”得到的奖励。因此,对于主观信任度的计算方法更新为式(3):

$$ST_{ij} = \frac{\alpha}{\alpha + \theta * \beta} \tag{3}$$

其中,θ 为惩罚因子,其取值通常大于 1。

由于车辆在行驶过程中处于动态变化的环境中,车辆之间历史交互信息的影响力将随着时间的变化而不断衰减,即使车辆处于不活动期间,其信任值也会随着时间的推移而降低。车辆的历史信任值与当前计算获得的最新信任值之间的聚合更新方式为式(4):

$$ST_{ij} = u * ST_{ij}^{old} + (1 - u) * ST_{ij}^{new} \tag{4}$$

其中,u 为信任度衰减因子,其取值范围是[0,1]。

2.2 推荐信任计算

如果网络中的两个车辆之前没有任何数据交互或者其他形式的合作,当二者首次通信建立信任关系时需要参考周围其他“邻居”车辆提供的推荐信息,通过这种方式获取的信任被称为“推荐信任”或者“间接信任”。推荐信任的传播可以通过允许车辆感知多个来源提供的推荐信息来预测以前从未交互的车辆的可信度,从而提高信任计算的覆盖率和准确率。在计算推荐信任度时,本文仅采纳评估节点 1-跳范围内的邻居节点提供的推荐信息,以此来降低计算过程的复杂度。在反馈推荐信任的过程中,某些恶意车辆可能会故意给出较低的信任值,当推荐车辆节点个数较多时,一个低信任推荐可能对节点的总体评估影响不大,但当多个恶意车辆合谋给出低推荐信任时,被评估节点的信任度就会受到较大影响。为抵御恶意节点在推荐过程中采取的差评攻击和选票攻击,本文采用一种动态聚类算法将推荐信息进行分类处理,预先排除可信度很低的推荐信任,有效抵制恶意车辆节点的串通攻击,提高推荐信任计算的准确度。

该动态聚类算法通过最大化包含在评估节点邻域中的信息,去除推荐信息中偏离度较大的数据,从而减少错误估计对计算推荐信任值造成的影响。该算法根据以下参考指标对推荐信息进行聚类处理。

2.2.1 车辆之间的亲密度

车辆在行驶过程中需要不断的与其他车辆进行数据传输和共享,因此车辆之间交互的次数从一定程度上能够反映出二者之间的亲密程度,进而可以根据其亲密程度来选择是否接受对方提供的推荐信息。大多数情况下我们都会愿意相信自己“熟悉”的人所提供的信息,而对“陌生人”则心怀警惕。如果评估车辆与推荐车辆交互次数有限,则对方提供的推荐信息具有很大的随机性;相反,如果二者之间交互频繁,则对方提供的推荐信息具有较强的确定性。通过计算节点间的亲密度并与预定义的阈值进行对比,可以有效过滤掉那些不确定信息,为后续其他环节的分析处理工作提供了必要的保障。假设车辆 i 的 n 个邻居分别为 $\{V_1, V_2, \cdots, V_n\}$,那么车辆 i 与其中一个邻居车辆 r 之间的亲密度计算如式(5):

$$V_{ir}^{interaction} = \frac{\alpha_{ir} + \beta_{ir}}{\sum_{j=1}^{n}(\alpha_{ij} + \beta_{ij})} \tag{5}$$

2.2.2 推荐信任的偏差度

偏差度主要体现了客观推荐信任与主观经验之间的兼容程度。网络中的每辆车都会将邻居发送的推荐信任度与自己通过直接交互计算得出的主观信任度进行对比,最终仅保留与自身判断没有太大偏差的推荐信息。通过将偏差度计算结果与预定义的偏差阈值进行比较,可以有效排除与评估节点自身信息存在较大差异的任何推荐信息。假设对于同一辆车 k 而言,评估车辆 i 计算的主观可信度为 ST_{ik},推荐车辆 r 提供的推荐可信度为 RT_{rk},二者之间的偏差度计算如式(6):

$$V_{ir}^{deviation} = | ST_{ik} - RT_{rk} | \tag{6}$$

2.2.3 车辆之间的地理关联度

车辆的行驶路线往往会受到当前路网信息的约束,此外,道路两侧的建筑物也会对车辆之间的无线通信产生较大的影响。为了保证车辆间的通信质量,防止由于外界干扰导致信息失真的情况发生,通常会根据车辆之间的物理距离、转发跳数及传输延迟等指标来计算评估节点与推荐节点之间的地理关联度,本文根据车辆之间的欧氏距离作为地理关联度的评判数据。假设评估车辆 i 和推荐车辆 r 的位置信息分别是 (x_i, y_i) 和 (x_r, y_r),二者之间的地理关联度计算如式(7):

$$V_{ir}^{correlation} = \sqrt{(x_i - x_r)^2 + (y_i - y_r)^2} \tag{7}$$

利用动态聚类算法对邻居车辆提供的推荐信息进行过滤筛选的流程如图 2 所示。通过去除这些存在一定的偏差且随机性较大的干扰信息,最终获取有效的推荐信息。假设评估车辆 i 收到周围 n 个邻居提供的关于车辆 j 的推荐信息后,对于车辆 j 的推荐信任度计算方法如式(8):

$$RT_{ij} = \sum_{r=1}^{n} \left(\frac{\alpha_{ir} + \beta_{ir}}{\sum_{k=1}^{n}(\alpha_{ik} + \beta_{ik})} * ST_{rj} \right) \tag{8}$$

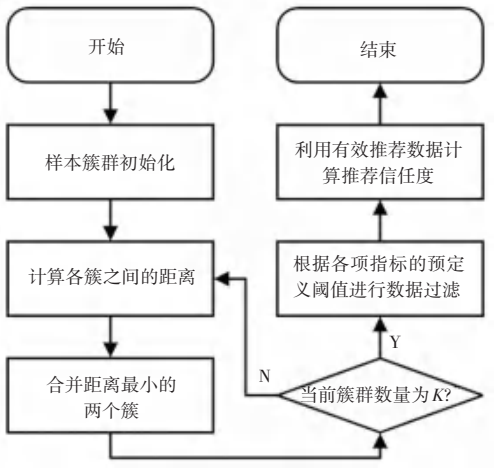

图 2　动态聚类流程图

Fig. 2　Flow chart of dynamic clustering

2.3　全局信任计算

鉴于车辆的高速移动特性及车辆之间交互的有限性和随机性，为了提高信任度计算的准确性，本文综合考虑评估车辆自发产生的主观信任和周围邻居提供的推荐信任，最终获得被评估车辆的全局信任，计算方法如式(9)：

$$GT_{ij} = \omega * ST_{ij} + (1 - \omega) * RT_{ij} \qquad (9)$$

其中，ω 是权重因子，关系到主观判断和客观推荐对于全局信任的影响程度，取值范围是[0,1]。

3　实验仿真及结果分析

本文实验仿真的核心目标主要包括：

(1)针对高速移动中的车辆展开动态信任度评估，其评估结果应具有较高的准确度；

(2)当周围环境中存在一定比例的恶意攻击车辆时，信任计算模型应具有较强的抗攻击性和鲁棒性。

在实验过程中，本文使用了 Veins 模拟仿真平台，这是一个广泛用于车辆网络模拟的开源框架。Veins 仿真平台包含了两个独立的模拟器：SUMO 和 OMNET++。SUMO 是专用的交通仿真模拟器，可以在虚拟地图上模拟不同的交通模式及车辆移动特性。既可以从开源网站 OpenStreetMap 导入地图数据，也能够利用 XML 文件进行自定义路网设计；OMNET++提供各种功能模块：应用层、DSRC 和物理层，以确保真实的网络行为。OMNET++和 SUMO 之间利用开源框架 VEINS 提供的“交通控制接口(TraCI)”实现数据的离散式传输和共享。

本文在实验过程中使用了新乡市东区的部分路网数据，如图 3 所示。具体的实验仿真参数见表 1。

图 3　新乡市东区路网信息

Fig. 3　Road Network Information about the Eastern District of Xinxiang

表 1　仿真参数

Tab. 1　Simulation parameters

参数	值
仿真区域	1 000 m * 3 000 m
汽车数量	200 辆
通信范围	100 m
攻击者数量	50 辆
车速	0~50 km/h
仿真时间	1 200 s

在实验过程中，选取当前信任管理领域中具有重要代表地位的“投票法”作为对比方案，从以下 3 个方面对本文提出的信任管理模型进行仿真验证。

3.1　信任模型的性能

为了测试信任模型的相关性能，本文在实验过程中使用了 3 个技术指标：①识别率；②假阴性；③假阳性。识别率反映出了信任模型的有效性，即：能够甄别出正常车辆和恶意车辆，保证其在行驶过程中可以采取正确决策，提高交通安全；而假阴性和假阳性则体现了信任计算结果的“误报”情况，将导致车辆行驶过程中存在一定的安全隐患。本文提出的信任模型可以有效地过滤信任计算过程中的干扰信息，具有较高的识别率和较低的误报率，信任模型性能测试结果如图 4 所示；基于“投票法”的信任模型在网络中不存在恶意攻击者的情况下能够做出较为准确地判断，但随着攻击者比例的增加，车辆接收到的干扰信息逐渐增多，导致信任度计算结果的准确性逐步下降，误报率不断升高，最终影响到 VANET 的正常运行，如图 5 所示。

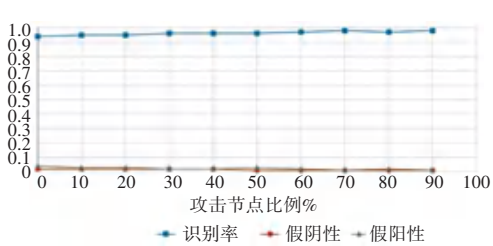

图 4　信任模型性能测试

Fig. 4　Performance testing of trust model

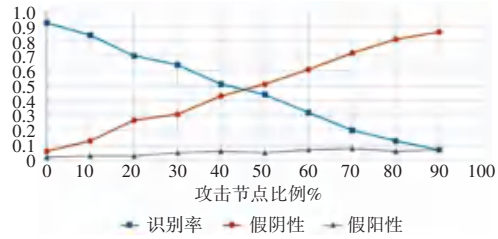

图 5 “投票法”模型性能测试

Fig. 5 Performance testing of “voting method” model

3.2 信任模型的抗攻击性

“差评攻击”和“投票攻击”是 VANET 应用中常见的两种攻击模式,恶意车辆通过发动相关攻击,给评估节点提供错误的推荐信息,从而导致信任度的计算结果失真。在实验过程中,分别选取一个正常车辆和一个恶意车辆,观察二者在不同模型中的信任度的变化趋势。相邻节点中随着攻击者数量的增多,评估节点会接收到越来越多不真实的信任度推荐如图 6 和图 7 所示。本文提出的信任模型通过将所有的推荐信息分簇聚类并与评估者本身做出的主观判断进行对比,能够很大程度上屏蔽“失真评价”带来的干扰,推荐信任度的计算结果较为稳定地维持在一个与实际情况相符的水平;而“投票法”信任模型中,随着攻击者比例的增大,恶意节点拥有越来越多的“话语权”和“影响力”,致使信任度的计算结果与实际情况存在较大的偏差。由此可知,本文提出的信任模型具有较强的抗攻击性和鲁棒性。

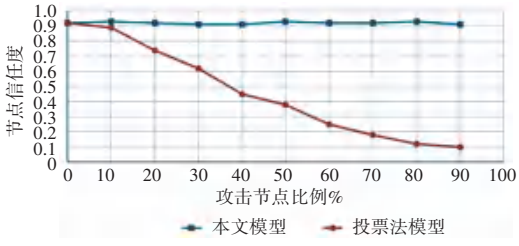

图 6 正常节点的信任度变化

Fig. 6 Trust variation of normal nodes

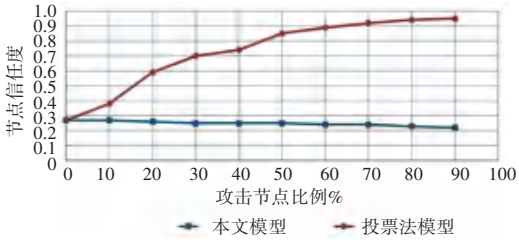

图 7 恶意节点的信任度变化

Fig. 7 Trust variation of malicious nodes

3.3 网络性能

整个 VANET 的性能评估主要与两个参数指标有关:网络吞吐量和丢包率。

图 8 和图 9 展示了两种不同的信任模型中网络的吞吐量和丢包率随着攻击节点比例的增加对应的变化趋势。当网络中所有节点都处于正常工作状态时,两种信任模型对应的网络性能基本保持一致。随着攻击节点的比例增大,在基于“投票法”的信任模型中攻击节点的影响力将会逐渐提高,使得信任计算过程产生混淆,对被评估节点的信任度计算结果产生较大的干扰,最终致使网络的吞吐量由 85% 下降到不足 30%,丢包率由 26%上升至 95%。本文提出的信任模型中,攻击节点比例的增加尽管也会对信任计算过程产生干扰,但同时也导致这种群体攻击行为更加的特点鲜明,通过对推荐信息进行了动态分层过滤,能够有效的甄别周围邻居中存在的攻击者,从而保证整个网络长期处于高吞吐量及低丢包率的稳定工作状态。

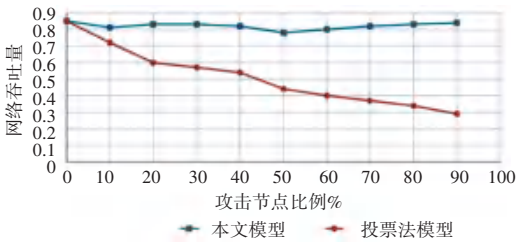

图 8 网络吞吐量测试

Fig. 8 Testing of network throughput

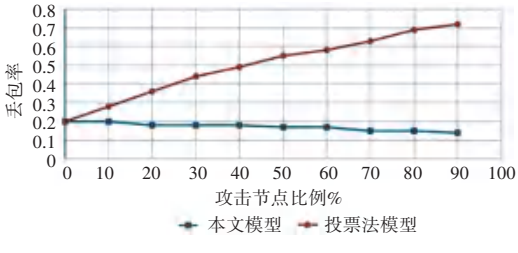

图 9 丢包率测试

Fig. 9 Testing of Packet drop rate

4 结束语

本文通过分析 VANET 通信过程中存在的安全隐患,针对内部节点的攻击行为提出了一种基于动态聚类的信任计算模型。该模型根据车辆当前的行驶环境及相邻车辆之间的交互数据,动态地滤除恶意攻击者发布的干扰信息,从而综合计算出被评估车辆的真实信任度。实验结果表明,本文设计的信任模型具有较高的准确率及较低的误报率,能够有效的识别出 VANET 中存在的恶意攻击者,为车辆后续的行为决策提供了有力的安全保障。即便随着

恶意攻击者的数量不断增多，该模型的信任计算结果始终保持在一个与实际情况相符的水平，具有较强的抗攻击性和鲁棒性。同时，整个网络也能长期保持较高的吞吐量和较低的丢包率。

参考文献

[1] AHMED A, BAKAR K A, CHANNA M I, et al. TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network [J]. IEEE Sensors Journal, 2015,15(12):6962-6972.

[2] CHENG Y, FU X, DU X, et al. A lightweight live memory forensic approach based on hardware virtualization[J]. Information Sciences, 2017,379:23-41.

[3] CHO J, SWAMI A, CHEN I. A Survey on Trust Management for Mobile Ad Hoc Networks[J]. IEEE Communications Survey & Tutorials, 2011,13(4):562-583.

[4] HU H, LU R, ZHANG Z, et al. REPLACE: A reliable trust-based platoon service recommendation scheme in VANET[J]. IEEE Transactions on Vehicular Technology, 2017,66(2), 1786-1797.

[5] WU W, LI R, XIE G et al. A Survey of Intrusion Detection for In-Vehicle Networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2020,21(3): 919-933.

[6] LIU Z, WENG J, MA J, et al. TCEMD: A Trust Cascading-Based Emergency Message Dissemination Model in VANETs[J]. IEEE Internet of Things Journal, 2020,7(5):4028-4048.

[7] 李馥娟,王群,钱焕延. 车联网安全威胁综述[J]. 电子技术应用,2017,43(5):29-33,37.

[8] AHMAD F, KURUGOLLU F, ADNANE A, et al. MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles[J]. IEEE Internet of Things Journal, 2020,7(4):3310-3322.

[9] 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, 2020, 22(5): 2553-2571.

[10] Aljawharah Alnasser, SUN Hongjian, JIANG Jing. Recommendation-Based Trust Model for Vehicle-to-Everything(V2X)[J]. IEEE Internet of Things Journal, 2020,7(1):440-450.

[11] CHEN Y, WEI Y. A beacon-based trust management system for enhancing user centric location privacy in VANETs[J]. Communications and Networks, 2013,15(2):153-163.

[12] H. Al Falasi, N. Mohame. Similarity-based trust management system for detecting fake safety messages in vanets[C]// International conference on internet of vehicles. Springer. 2015: 273-284.

[13] CHEN J, MAO G, LI C, et al. A Topological Approach to Secure Message Dissemination in Vehicular Networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2020,21(1): 135-148.

[14] HASROUN H, SAMHAT A, BASSIL B, et al. Trust model for secure group leader-based communications in VANET[J]. Wireless Networks, 2019,25:4639-4661.

[15] 樊娜, 段宗涛, 王青龙,等. 面向车辆网环境的车辆行为可信决策机制[J]. 计算机工程与设计, 2018,39(1):35-37,43.

(上接第 173 页)

色 RGB(0,127,256)；网格精度为 256 * 256；海浪强度 0.2；水流速度 0.2；水流方向 0；水浪大小 10；光源方向 50。

为了对比 Perlin 噪声算法的效果，还选用了随机点生成高度进行实验，除生成高度算法不同，其它参数(网格精度、海浪强度、水流速度、水流方向等)都与 perlin 噪声算法的海面模拟相同。

实验程序运行结果如图 3 所示。其中，图 3(a)为随机点生成高度的海面仿真的结果图，图 3(b)为经过柏林噪声生成高度的海面仿真结果图。图 3(b)模拟海面的参数包括：模拟范围、海水颜色、网格精度、海浪强度、水流速度、水流方向、水浪大小、光源方向等。把这些用于控制海浪效果的数值参数化，以 GUI 的形式展示出来，更加直观。

(a) 随机点生成高度的海面仿真结果　　(b) 经过柏林噪声生成高度的海面仿真结果

图 3　仿真结果

Fig. 3　Simulation results

通过对比图 3(a)和图 3(b)，可以很直观的看出，图 3(b)经过柏林噪声生成高度的海面仿真，更加接近真实的海面，避免了浪尖处易失真的问题。

4　结束语

本文主要从海面高度场的生成和海面网格建模，对海面仿真进行研究分析。虽然每一个模块的完成都兼顾海面的真实感和实时性，但离真实的海面场景还有一定的差距(如：天气情况和海面漂浮物对海面场景的影响等问题)，有待进一步研究。

参考文献

[1] 吴园园. 海洋环境的可视化仿真平台设计与实现[D]. 呼和浩特：内蒙古大学,2016.

[2] 柳有权,刘学慧,朱红斌,等. 基于物理的流体模拟动画综述[J]. 计算机辅助设计与图形学学报,2005(12):2581-2589.

[3] 张维. 海洋场景绘制关键技术研究及实现[J]. 实验科学与技术,2016,14(5):52-55.

[4] 石秋华,孙娟. 利用 Perlin 噪声生成水波面的动态模拟研究[J]. 软件导刊,2012,11(2):140-142.

[5] 瞿师,李苏军,吴玲达. 数字地球上的海面建模与绘制技术研究[J]. 系统仿真学报,2008,20(S1):334-336,340.