

DOI: 10.7652/xjtuxb201502012

车载自组网中联盟博弈的虚假数据检测策略

刘伎昭, 王泉

(西安电子科技大学计算机学院, 710071, 西安)

摘要: 针对车载自组网(vehicular ad-hoc network, VANET)中多个恶意节点合谋的虚假数据攻击问题,提出了联盟博弈的虚假数据检测策略。该策略利用合作节点测量的无线信号强度进行交叉位置验证,发现伪造位置的恶意节点及其注入的虚假信息。为降低节点自私行为对检测准确性的影响,提出了满足“核”分配条件的收益分配函数激励节点加入联盟;证明了该函数满足个体理性条件和有效性条件,节点的最优策略是选择合作,形成的联盟具有稳定性。仿真结果表明:该策略能够有效激励节点合作,降低无线信号强度的随机偏差对位置验证准确性的影响,获得了超过90%的虚假位置检测率,并进一步增强了系统的抗合谋攻击能力,在不同的恶意节点比例下虚假告警消息检测率比基于表决的攻击者本地驱逐协议(local eviction of attackers by voting evaluators, LEAVE)提高了69.3%。

关键词: 车载自组网;虚假数据检测;合作博弈;联盟博弈

中图分类号: TN929.5 **文献标志码:** A **文章编号:** 0253-987X(2015)02-0069-05

A False Data Detecting Scheme Based on Coalition Game for Vehicular Ad-hoc Networks

LIU Jizhao, WANG Quan

(School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

Abstract: A false data detecting scheme based on coalition game is proposed to focus on collusive false data attack problem in vehicular ad-hoc networks (VANET). The proposed scheme uses the measured radio signal strength at cooperative nodes to perform the position cross-check and to detect the malicious nodes with false position and the false information injected by them. A payoff allocation function that satisfies the “core” allocation condition is proposed for stimulating nodes to join coalitions so that the impact of selfish behaviors of nodes on the accuracy of detecting can be reduced. It is proved that the proposed payoff allocation function satisfies an individual rational condition and an efficiency condition, and that the best strategy of nodes is to cooperate with each others and the formed coalition has the stability feature. Simulation results show that the proposed scheme can effectively stimulate nodes to cooperate, and reduce the impact of random deviation of radio signal strength on the accuracy of position verification. The detecting ratio of false positions is more than 90%. Furthermore, the ability for resisting collusive attacks is enhanced. A comparison with the LEAVE protocol show that the proposed scheme increases the detecting rate of false alert messages by 69.3% under various proportions of malicious nodes.

Keywords: vehicular ad-hoc networks; false data detection; cooperative game; coalition game

收稿日期: 2014-08-13。 作者简介: 刘伎昭(1981—),男,博士生;王泉(通信作者),男,教授,博士生导师。 基金项目: 国家自然科学基金资助项目(61100153, U1135002)。

网络出版时间: 2015-01-06

网络出版地址: <http://www.cnki.net/kcms/detail/61.1069.T.20150106.1759.001.html>

车载自组网^[1] (vehicular ad-hoc network, VANET)是安装在车辆上的无线节点(on board unit, OBU)和部署在路边的基础设施(road side unit, RSU)组成的自组织异构多跳无线网络,是未来智能交通系统的关键技术。VANET中OBU通过车载传感器感知车辆的位置、速度、加速度等信息,利用无线自组织网络技术交换、聚合和分发这些信息,从而实现事故告警、协作驾驶等多种应用^[2]。

出于节点自私性、传感器故障或恶意攻击等多种原因,VANET中OBU可能发送不准确,甚至虚假信息。例如错误的车辆位置、伪造的告警信息等^[3]。由于攻击者一般为网络合法节点,能够产生合法的消息签名^[4],现有的基于消息和实体认证的VANET安全机制^[5-6]难以有效检测和抵御此类攻击。文献[7]提出了基于轨迹的检测方法,通过检测目标车辆的位置、移动轨迹与报告的交通事件之间是否存在矛盾判断告警消息的真实性,例如交通事件超出车辆的观测范围、车辆速度异常(超过300 km/h)、发出道路拥堵通告的车辆却高速行驶等。Raya等提出了多节点合作的检测方法,节点统计邻居节点提供的数据并将显著偏离均值的数据视为虚假数据,通过对嫌疑节点发起指控和迭代的节点可信度计算发现不端节点^[8]。文献[9-10]提出了合作的位置验证方法,节点通过测量接收的无线信号强度(radio signal strength, RSS)估计与邻居节点之间的相对距离,通过三角定位法计算节点真实位置。由于VANET中节点属于不同的利益主体,具有自私性和自治性,出于自身利益考虑节点可能不合作,造成“搭便车”现象并导致检测率的降低,而上述合作检测方法都没有考虑自私节点问题。此外,如果网络中存在合谋的恶意节点,通过注入虚假观测数据的方法攻击检测系统,也能影响检测准确性。

本文提出了联盟博弈的VANET合作虚假数据检测策略。节点基于接收信号强度估计与邻居节点的距离,多个节点形成联盟进行交叉位置验证,评判节点位置真实性,检测伪造虚假位置的恶意节点及其提交的虚假观测信息,增强检测系统的抗合谋攻击能力。提出的激励策略根据节点在联盟形成中的作用决定收益分配比例,基于“核”概念分析了联盟的稳定性,证明了节点加入联盟能够增加自己的收益,所有节点参与的“大联盟”能够实现个体收益的最大化,任何节点子集无法通过分裂联盟提高收益水平。

1 系统模型

1.1 网络模型

VANET由车辆节点、路边基础设施和认证中心组成。本文涉及两种类型的消息:beacon消息和告警消息。车辆节点周期性地广播beacon消息向邻居车辆报告自己的位置、速度、加速度、方向等运动状态信息,广播间隔为100~300 ms。在发生紧急交通事件时,车辆节点发送包含事件类型、位置、时间等信息的告警消息^[11]。

1.2 联盟博弈模型

使用联盟博弈^[12]建模多个理性的自治主体之间彼此协作增加各自收益的行为。联盟博弈定义如下。

定义1 联盟博弈是一个有序对 $\langle N, v \rangle$,其中 N 是参与者集合, $v:2^N \rightarrow R$ 是满足 $v(\emptyset)=0$ 的特征函数。实值函数 $v(S)$ 是多个参与者彼此合作结成联盟 S 时,联盟成员获得的收益。所有参与者组成的联盟称为大联盟,记为 N 。大联盟的收益记为 $v(N)$ 。

定义2 在 n 人联盟博弈 $\langle N, v \rangle$ 中,设 $x=x_1, x_2, \dots, x_n$ 是一个 n 维向量,满足下面两个条件

$$x_i \geq v(\{i\}), i=1, 2, \dots, n \quad (1)$$

$$\sum_{i=1}^n x_i = v(N) \quad (2)$$

x 称为一个分配。全体分配称为分配集,记为 $I(N, v)$ 。式(1)为个体理性条件,即任何一个参与人加入联盟分配到的收益应该不小于独自行动得到的收益。式(2)为有效性条件,即所有收益都被分配没有剩余。

定义3 设 $\langle N, v \rangle$ 是一个 n 人合作博弈,若存在一个分配 $x=x_1, x_2, \dots, x_n \in I(N, v)$,使得对所有 $S \subseteq N$,满足

$$v(S) \leq \sum_{i \in S} x_i \quad (3)$$

这种分配 x 组成的集合称为博弈的核,记为 $C(v)$ 。利用式(3)对分配方案是否为核的检验过程称为独立性检验。核中的分配意味着不存在参与人或参与人组合能够从大联盟中分裂出去以获得更高的收益,即大联盟是稳定的。

2 联盟博弈的虚假数据检测策略

本文假设的多恶意节点合谋虚假数据攻击场景如图1所示,恶意节点1为了获得更快的通行速度,发送虚假的交通事故告警消息声称车辆4发生了交通事故,从而诱导前方车辆2驶出当前道路。事件

观测范围内的节点可以通过投票方式判断告警消息的真实性。由于节点3和6是诚实节点,因此虚假告警消息可成功检出,但事件观测范围之外的合谋节点1和5通过声称虚假位置将自己伪装为观测节点参与投票,能够影响投票结果使受害节点2相信虚假的交通事件。

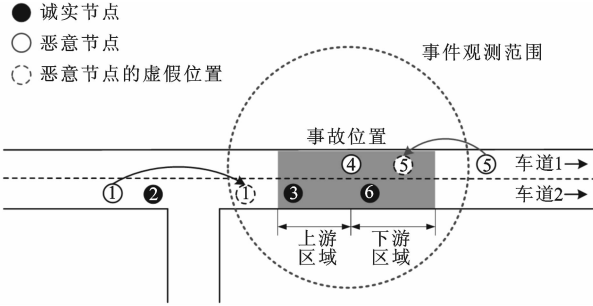


图1 合谋攻击场景

本文使用节点合作机制增强检测系统的抗合谋攻击能力。节点合作包括两个方面:首先,每个观测节点通过测量接收信号强度估计与邻居节点的相对距离,多个节点彼此合作进行交叉位置验证,可以发现伪造虚假位置的恶意节点;其次,节点彼此合作收集目标区域内车辆运动状态信息,通过检测交通流异常判断告警消息的真实性,例如交通事故的发生会造成车道阻塞,上游区域内车辆减速、变道至邻近车道,下游区域内车辆将会做出加速、变道回原车道等动作。

2.1 检测过程

任意接收到告警消息的车辆可以发送检测请求发起合作的虚假数据检测,发送请求的车辆称为检测车辆。检测请求指定了事件的类型、位置和发生时间,通过安全组播路由协议转发到观测范围内所有观测车辆。

步骤1 证词采集。通过监测目标区域内车辆的运动参数发现异常车辆。使用随机变量 V 和 A 表示正常通行状态下车辆的速度和加速度,假设其分布为已知,定义目标车辆异常低速为速度 $v < v_\lambda$,异常减速为车辆加速度 $a < a_\lambda^-$,异常加速为车辆加速度 $a > a_\lambda^+$,其中 v_λ 、 a_λ^- 和 a_λ^+ 是判断车辆速度、加速度出现异常的阈值,计算方法如下。

$$P[v < v_\lambda] < \lambda \quad (4)$$

$$P[a < a_\lambda^-] < \lambda \quad (5)$$

$$P[a > a_\lambda^+] < \lambda \quad (6)$$

式中: λ 是显著性水平。式(4)~(6)分别表示正常通行状态下车辆速度 v 低于 v_λ 、加速度 a 低于 a_λ^- (高于 a_λ^+) 的概率小于 λ 。观测车辆使用异常车辆

beacon 消息生成 beacon 证词,同时测量所有邻居车辆的 beacon 消息接收信号强度生成位置证词。

步骤2 位置验证。检测节点收集观测节点的证词后,首先验证观测节点位置的真实性。针对观测节点 j 的验证过程如下: j 的声称位置记为 p_j , j 与任意邻居 i 的欧氏距离 $\|p_i, p_j\|$ 记为 d_{ij} ,使用阴影衰落模型计算节点 i 针对节点 j 的理论接收信号强度

$$s_m = -10\beta \log(d_{ij}) + X \quad (7)$$

式中: β 是路径衰落指数; X 是服从正态分布的随机变量,其均值为 0,标准差为 σ 。如果理论信号强度 s_m 与节点 i 测量的实际信号强度 s_i 满足

$$|s_i - s_m| < \delta \quad (8)$$

即二者差值小于预定义的阈值 δ ,则认为节点 i 证实了位置 p_j 。如果超过半数的观测节点证实 j 的位置,则认为 j 的位置是真实的。针对检测出的虚假位置节点,检测节点丢弃该节点提交的所有 beacon 证词和所有涉及该节点的 beacon 证词。

步骤3 真实性判定。检测节点通过收集的 beacon 证词检测交通流异常。若上游区域内车辆异常减速概率、下游区域内车辆异常加速概率以及上/下游区域内车辆异常低速概率均超过相应的阈值,告警消息被判定为真,否则判定为假。

2.2 激励策略

使用虚拟现金激励节点合作。使用有向图 $G = (V, E)$ 表示节点合作关系。 V 是顶点集合,由 $N+1$ 个参与合作的车辆节点组成(N 个观测节点和 1 个检测节点),有向边 $e(i, j)$ 表示节点 i 为 j 提供了位置证词。 G 的基图 G' 中的连通分量称为联盟,任意节点有序对之间都存在有向边连接的完全有向图称为大联盟。通过提出的收益分配函数激励节点加入联盟。

在一次成功的检测过程中,认证中心为每个联盟 S 支付的虚拟现金数量为

$$v(S) = \delta(S)d(S) \quad (9)$$

式中: $d(S)$ 为联盟成员提交的 beacon 证词的数量; $\delta(S)$ 是支付因子,表示认证中心为一个 beacon 证词所支付的虚拟现金数量。 $\delta(S)$ 的计算方法为

$$\delta(S) = \sum_{i \in S} m_p(i) / \sum_{i \in N} m_p(i) \quad (10)$$

式中: $m_p(i)$ 指节点 i 提供的位置证词数量。在同时存在多个联盟的情况下,每个联盟获得的支付份额与联盟内位置证词的数量成比例。

联盟 S 中任意观测节点获得的分配为

$$x_i = \alpha m_b(i) + \beta m_p(i) \quad (11)$$

式中: $m_b(i)$ 为节点 i 提供的 beacon 证词的数量。

联盟 S 中检测节点获得的分配为

$$x_d = \delta(S)d(S) - (\alpha \sum_{i \in S - \{x_d\}} m_b(i) + \beta \sum_{i \in S - \{x_d\}} m_p(i)) \quad (12)$$

定理 1 提出的分配函数符合个体理性条件的充分条件是式(13)成立。

$$\max(\alpha, \beta) \leq \delta(S)d(S) / \sum_{i \in S} m_b(i) + \sum_{i \in S} m_p(i) \quad (13)$$

证明: 对于观测节点, 独自行动意味着只提供 beacon 证词, 不提供位置证词。按照收益分配函数, 独自行动节点所得分配为 0, 而式(11)中各项的值均为非负, 因此个体理性条件满足。对于检测节点, 有动机选择合作的条件为收益大于 0, 因此有

$$\begin{aligned} x_d = \delta(S)d(S) - (\alpha \sum_{i \in S - \{x_d\}} m_b(i) + \\ \beta \sum_{i \in S - \{x_d\}} m_p(i)) \geq \delta(S)d(S) - \max(\alpha, \beta) \cdot \\ (\sum_{i \in S - \{x_d\}} m_b(i) + \sum_{i \in S - \{x_d\}} m_p(i)) \geq 0 \end{aligned} \quad (14)$$

因此式(13)成立。证毕。

定理 2 提出的分配函数符合有效性条件。

证明:

$$\sum_{i \in S} x_i = x_d + \sum_{i \in S - \{x_d\}} x_i = v(S) \quad (15)$$

因此所有支付被分配没有剩余。证毕。

定理 3 提出的分配函数能够通过独立性检验, 因此该分配方案在核中。

证明: 假设大联盟形成, 观测节点数为 N , 每个节点的位置证词数目为 $N-1$, 大联盟获得全部的分配 $\delta(N)d(N)$ 。考虑任意联盟 S , 通过比较联盟 S 能够获得的收益分配 $v(S)$, 并将 $v(S)$ 与联盟 S 中所有节点加入大联盟获得的收益总额 $\sum_{i \in S} x_i$ 进行比较。如果 $\sum_{i \in S} x_i \geq v(S)$, 说明大联盟中没有任何节点子集能分裂出去以获得更高的收益。

$\forall S \subseteq N$, s. t. S 包含检测节点, 有

$$\begin{aligned} \sum_{i \in S} x_i - v(S) = \sum_{i \in S} m_d(i) / \sum_{i \in N} m_d(i) \delta(N)d(N) - \\ \sum_{i \in S} m_p(i) / \sum_{i \in N} m_p(i) \delta(S)d(S) = \\ \delta(N)d(N) - \delta(S)d(S) \geq 0 \end{aligned} \quad (16)$$

因此有 $\sum_{i \in S} x_i - v(S) > 0$, 提出的分配方案在核中。证毕。

从上述分析可以得出结论, 在给定的分配函数

下, 检测节点的最佳策略是发起检测请求, 合作节点的最佳策略是最大程度地合作, 即提交 beacon 证词并为其余 $N-1$ 个观测节点提供位置证词。

3 仿真与结果分析

使用交通仿真软件 SUMO 生成车辆移动轨迹, 道路拓扑基于 Openstreetmap 项目^[13]提供的西安市真实地理信息生成, 仿真区域大小为 $2 \text{ km} \times 2 \text{ km}$, 所有道路为双向, 每向 2 车道, 车辆密度为 50 辆/km。网络仿真器使用 NS-2 v2.35, 编译环境为 gcc 4.6.3, 仿真时间为 600 s, 节点无线传输距离为 300 m。节点虚假位置在距离真实位置 10~100 m 范围内随机选择。定义虚假位置检测率 p_t 为虚假车辆位置被成功检测的概率, 虚假位置误检率 p_f 为真实车辆位置被检测为虚假位置的概率, 虚假消息检测率 d_t 为虚假的告警消息被成功检测的概率。定义合作节点比例 φ 为观测范围内合作节点数目与诚实节点数目的比值, 自私节点比例 $\gamma = 1 - \varphi$, 恶意节点比例 η 为恶意节点数目与观测范围内总节点数的比值。

图 2 给出了本文方法的虚假位置检测率。考虑到真实交通环境中无线信号传播受环境影响较为明显, 造成实际信号接收强度与理论值偏差较大, 因此对阴影衰落模型中代表随机性偏差的随机变量 X 设置不同的标准差 σ , 评价检测率受影响的程度。仿真结果显示合作节点比例的增加能够显著提高检测率, 80% 的诚实节点选择合作时检测率为 50%~80%, 当 100% 诚实节点选择合作时, 即使在 $\sigma = 12 \text{ dB}$ 时也能获得超过 90% 的检测率。

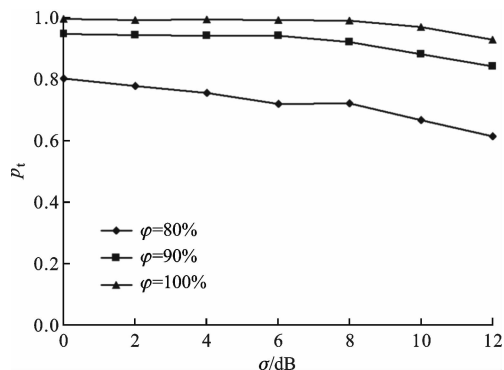


图 2 虚假位置检测率

图 3 给出了合作节点比例 φ 对虚假位置误检率的影响, 在 75% 的诚实节点选择合作时, 误检率为 18%, 这主要是由于较大的信号强度随机偏差使真实车辆位置被误检为虚假位置。随着合作节点比例

的增加,80%和 85%的诚实节点合作时误检率下降到 8%和 1%,说明合作节点数目的增加能够显著降低误检率。

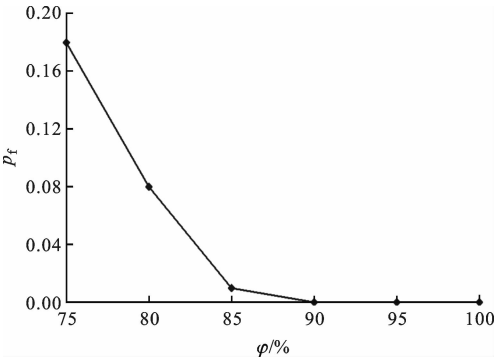


图 3 虚假位置误检率

图 4 给出了不同自私节点和恶意节点比例下的虚假告警消息检测率,并将本文方法与 Raya 等提出的 LEAVE 协议^[8]进行对比。假设本文提出的激励策略能使 90%的自私节点参与合作,从仿真结果可知:本文提出的激励策略能够减轻节点自私行为造成的负面影响,获得较高的检测率,即使存在 40%的自私节点,在恶意节点比例为 10%~30%时也能达到 87%~99%的检测率;由于 LEAVE 协议缺乏激励机制,节点不合作行为对检测率造成显著影响,当网络中自私节点的比例为 5%时,LEAVE 协议的检测率与本文方法接近,当自私节点比例达到 40%时本文方法的检测率显著高于 LEAVE 协议,本文方法的平均虚假告警消息检测率比 LEAVE 协议提高了 69.3%。

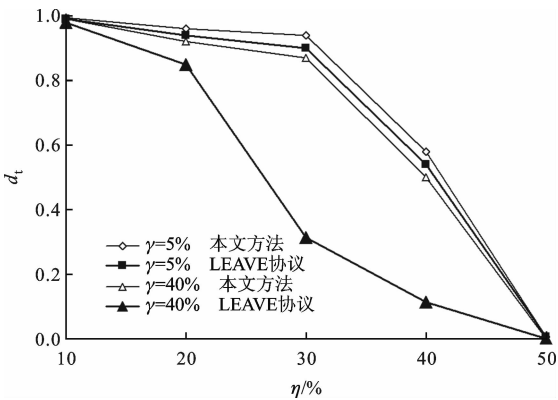


图 4 虚假消息检测率

4 结 论

VANET 节点具有自私性和自治性,在多节点合作的 VANET 合谋虚假数据攻击检测中,节点的“搭便车”行为能够显著影响检测准确性。针对虚假数据检测中的节点合作问题,本文首先建立了基于联盟博弈的节点合作关系模型,使用收益分配函数

激励节点参与合作;证明了该分配函数满足个体理性条件和有效性条件,节点的最优策略是加入联盟。仿真分析表明:该策略能够有效减轻自私节点对检测准确性造成的负面影响,获得较高的检测率;网络中存在 30%的恶意节点时,该策略能获得 87%的虚假告警消息检测率;与现有的 LEAVE 协议相比,虚假告警消息检测率提高了 69.3%。下一步工作中,我们计划采用数据聚合技术降低检测过程造成的通信负载和检测时延。

参考文献:

[1] LEE U, MAGISTRETTI E, GERLA M. Dissemination and harvesting of urban data using vehicular sensor platforms [J]. IEEE Transactions on Vehicular Technology, 2008, 58(2): 882-901.

[2] HARTENSTEIN H, LABERTAUX K P. A tutorial survey on vehicular ad hoc networks [J]. IEEE Communications Magazine, 2008, 46(6): 164-171.

[3] RAYA M, HUBAUX J P. Securing vehicular ad hoc networks [J]. Journal of Computer Security, 2007, 15(1): 39-68.

[4] 刘辉,李晖. 采用群组密钥管理的分布式车联网信息认证方案 [J]. 西安交通大学学报, 2013, 47(2): 58-62.

LIU Hui, LI Hui. A distributed authentication protocol for VANET [J]. Journal of Xi'an Jiaotong University, 2013, 47(2): 58-62.

[5] 郭建立,刘宏伟,吴智博,等. 面向信誉的自组网节点合作方法 [J]. 西安交通大学学报, 2009, 43(8): 17-21.

GUO Jianli, LIU Hongwei, WU Zhibo, et al. A new reputation-based cooperation enforcement scheme for MANETs [J]. Journal of Xi'an Jiaotong University, 2009, 43(8): 17-21.

[6] MERSHAD K, ARTAIL H. A framework for secure and efficient data acquisition in vehicular ad hoc networks [J]. IEEE Transactions on Vehicular Technology, 2013, 62(2): 536-551.

[7] RUJ S, CAVENAGHI M A, HUANG Zhen. On data-centric misbehavior detection in VANETs [C]// Proceedings of the 75th IEEE Vehicular Technology Conference. Piscataway, NJ, USA: IEEE, 2011: 1-5.

[8] RAYA M, PAPADIMITRATOS P, AAD I. Eviction of misbehaving and faulty nodes in vehicular networks [J]. IEEE Journal on Selected Areas in Communications, 2007, 25(8): 1557-1568.

(下转第 134 页)