一种车载自组织网络路况信息的数据信任模型

王光浩 吴 越
(上海交通大学信息安全工程学院 上海 200240)

摘 要 动态寻路是解决城市交通拥堵的重要手段。在动态寻路中,一些车辆产生和转发路况信息,使其他车辆能够避开拥堵路段。但一般车载自组织网络寻路算法缺乏验证路况信息的真实性的措施,导致恶意车辆能轻易篡改路况信息,误导其他车辆选择错误路线。提出了一种路况信息鉴别模型,该模型将基于数据的信任模型应用到路况信息真伪的鉴别中,并在一般投票算法的基础上利用D-S理论增加不确定情况下的鲁棒性。仿真实验表明,该算法在不增加额外信息交互的前提下,有效规避了恶意伪造信息,改进了车辆的行程时间。

关键词 动态寻路,基于数据的信任模型,Dempster-Shafer理论
中图法分类号 TP309.2 **文献标识码** A

Data Trust Model for Road Information in Vehicular Ad hoc Networks

WANG Guang-hao WU Yue
(School of Information Security Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

Abstract Dynamic routing is one of the solutions to urban traffic congestion problem. In dynamic routing plan, some vehicles are willing to produce and forward road information, so that other vehicles will analyze received information to avoid congested roads. Because of the lack of validation towards road information, malicious vehicles can tamper the road information in order to mislead other vehicles to choose the wrong route. A new trust model to verify road information was proposed. Validation towards the road information is based on data trust rather than entity trust. Dempster-Shafer theory is applied to voting algorithm to increase robustness in cases with uncertain. Simulation shows that with no additional data exchange, the model effectively detects and avoids malicious data. When looking for the right route according to route information from database, vehicles will not consider the malicious route information so that this model will help improve the vehicles' travel time.

Keywords Dynamic routing, Data trust, Dempster-Shafer theory

1 引言

城市交通问题一直是全球关注的重要问题。动态寻路(Dynamic Routing Plan)[1]是解决这一问题的手段之一,车辆利用本地的电子地图和从车载自组织网络中收集到的路况信息,动态地调整行驶路线,避开拥堵路段。一般车载自组织网络的研究着重于讨论如何有效转发路况信息,改善车辆行程时间,而对于车辆发送的路况信息本身的有效性和真实性不予鉴别。这给恶意节点篡改、伪造路况信息提供了便利,因此在车载自组织网络的路由算法中引入信任算法对于改善一般寻路算法的鲁棒性有重要意义。

在Ad hoc网络中,常见信任模型[2]描述信任一般针对每个实体(车辆)。这种信任的评估一般有3类途径:对实体间交互的观测、利用时间衰减以及不同实体间信任列表的交换。但是在车载自组织网络中,基于实体的信任模式存在很多问题。车辆之间再次相遇的概率较低,基于实体间交互观测到的信任难以取得足够数据,容易造成误解;计算路径时对路况信息有较高的实时性要求,利用时间来衰减信任难以提供良好的实时性;车辆在道路上会遇到相当数量的其他车辆,维护信任列表的开销过大。

大部分车载自组织网络动态寻路算法都利用路况信息进行寻路,因此直接利用基于数据的信任模型来判断路况信息的有效性,相比实体信任模式在判断出实体是否可信后,再判断其提供的路况信息的有效性更加简单有效。同时,基于数据的信任模型不需要引入过多额外的信息交换,减少了车辆之间的通信开销,也不存在基于实体信任的诸多问题,适用于验证路况信息的有效性。

本文针对车载自组织网络中动态寻路算法的路况信息安全性问题,将基于数据的信任模型运用到路况信息鉴别上。该算法在判断道路信息有效性时,采用Dempster-Shafer理论(简称D-S理论)[3]描述信任,并用投票算法进行统计,因此称为"基于数据信任的路况信息鉴别模型"(Road Information Data-Trust Model,简称RIDTM)。实验表明,RIDTM在常规车载自组织网络中,能够有效鉴别存疑的路况信息。

本文第2节介绍目前已有的与车载自组织网络信任模型相关的研究成果;第3节描述RIDTM的具体算法;第4节讨

到稿日期:2013-08-31 返修日期:2013-10-28 本文受国家自然科学基金项目(60932003,61271220,61211130104)资助。
王光浩(1989-),男,硕士生,主要研究方向为车载自组织网络、机会网络安全,E-mail:grayeva@sjtu.edu.cn;吴 越(1968-),男,博士,副教授,主要研究方向为无线网络安全。

论仿真实验的场景和实验结果；最后总结全文。

2 研究现状

Ad hoc 网络中对信任的研究有很长的历史。Eschenauer 等人[4]介绍了 MANET 中建立信任的基本原则，并同常规因特网进行了比较。其描述了一般证据的产生方式，以及在以节点为中心的认证模式中的分配方法。Sun 等人[5]的主要观点是信任的不确定性可以用熵来计算，同时引入了信心(Confidence of Belief)的概念来区分长期和短期信任。Theodorakopoulos 和 Baras[6]认为信任的传递可以不依赖于过去的信息交互，他们将信任评估建模成一个有向图的路径问题，利用路由协议来计算信任。

文献[7-10]都利用贝叶斯方法(Bayesian Inference，简称 BI)来构造声望信任系统，其基于间接信息产生针对实体的信任。而文献[2]提出一种直接基于数据的信任模型，利用本地采集数据和预先设定的信任矩阵来产生信任评价。一般，声望信任系统中节点信任值的计算需要观测节点间的交互，而基于数据的信任更加关注于数据本身。在此基础上，Marcela[11]等人提出的 DECADE 模型利用非合作式博弈来实现节点间的合作并孤立恶意节点。Aifeng[12]等人提出基于数据信任的 RATE 算法，利用路侧节点(Road Side Unit，简称 RSU)来辅助信任建立，并利用蚁群算法优化了算法效率。TRIP 协议[13]利用实体和数据信任的混合模式，根据直接邻居、间接邻居和认证中心等多个信息来源，对信息进行分级的信任处理。

相比 BI，D-S 理论在表达不确定性(Uncertainty)和度量上灵活简便，推理机制也非常直观，在信息不确定度较高情况下具有更好的鲁棒性。目前，D-S 理论在 Ad hoc 网络中的应用并不多。Jøsang[14]的工作中出现了 D-S 理论中的信任、不信任和不确定的概念，其描述了一个基于主观逻辑的认证代数方法。Chen 和 Venkataramanan[15]研究了如何在 Ad hoc 网络的分布式入侵检测中应用 D-S 理论。Siaterlis 和 Maglaris[16]将 D-S 理论应用到 DoS 异常检测中。

投票机制在基于数据的信任模型中常常被采用。Jiang 和 Baras[17]的方法基于本地投票对投票进行加权求和。但是一般加权求和时，相互冲突的投票会中和掉，而应用 D-S 理论则会导致更大的不确定性。Ostermaier 等人[18]实例化了基于数据信任模型，分析了投票方案处理本地危险警告的性能。

3 模型详述

3.1 场景假设

一般车载自组织网络中，城市地图被建模成一张有向加权图。其中每一条边关系到一个通行时间(Travel Time)，该值反映了车辆经过该路段时所用的时间。车辆在道路上行驶的过程中会产生路况信息，其中主要包括路段 ID 和车辆在该路段上的行程时间。这些信息通过无线信道在网络中传播，其他车辆收到这些信息，就会用信息中的行程时间更新本地地图中对应道路的权值，并重新计算行车路线。

对于缺乏安全保护的路况信息，常见的攻击形式有消息伪造攻击、消息重放攻击、消息完整性攻击、身份假冒、DoS 攻击以及针对隐私的路径追踪等等[19]。本文着重于讨论消息伪造攻击，伪造的方式是车辆将发送路况信息中的行程时间进行恶意的夸大或者缩小，以此来误导其他车辆进行错误的路由选择。

在本文的场景中，车辆被分为 4 类，如表 1 所列。

表 1 车辆类型

车辆类型	说明
未装备车	车辆没有装备通信装置，车辆只能按照预定路线行驶，不会根据其他车辆提供的路况信息改变
恶意车辆	车辆发送路况信息时会修改行程时间。它们会根据收到的路况信息进行寻路
受信车辆	车辆发送的数据得到其他车辆的信任。它们会无私地参加信息的广播和转发，一般为公交车辆或是政府车辆
一般车辆	车辆会接收和发送路况信息，也会根据收到的路况信息进行寻路。是一般车载自组织网络中最一般的参与者

3.2 路况信息格式

在车载自组织网络中，车辆很难实时地和 PKI 进行通信，因此难以用常规的认证方式进行数据认证。一般用身份密码(Identity Based Cryptography，简称 IBC)[20]的方式解决这一难题。利用身份密码，车辆可由私钥产生中心(Private Key Generator，简称 PKG)分配的密钥进行数据包的签名，其他车辆用信息中的 ID 便可验证数据和身份的有效性。

因此，每条路况信息格式如下：

$$M_j^i:\{v_i,l_j,t_j^i,timestamp,sign(m,v_i)\} \tag{1}$$

其中，m 表示$\{v_i,l_j,t_j^i,timestamp\}$。$v_i$ 表示 ID 为 i 的车辆，l_j 表示 ID 为 j 的路段，t_j^i 表示车辆 i 在路段 j 上花费的行程时间，$timestamp$ 表示 M 产生的时间戳。$sign(m,v_i)$ 表示利用 v_i 的私钥对消息 m 进行身份密码签名。

其他车辆需要区分发送车辆是否为可信车辆，因此 PKG 在分配车辆 ID(身份密码)和密钥时，可在 ID 中设计车辆受信的标志位。若引入了隐私匿名设计，则受信车辆通常不需要进行匿名处理，一般车辆可以直接分析车辆是否匿名来判断其受信与否。

3.3 信息接收流程

本地数据库 M_{recv} 以$\{l_j,v_i,M_j^i\}$的数据格式保存路况信息，在收到新的路况信息时进行更新操作：

1. 验证信息的签名完整性并且符合 v_i 时进入步骤 2；否则拒绝数据包。

2. 判断本地是否存在相同 l_j 和 v_i 对应的记录，如没有，则在本地数据库中新建；否则进行步骤 3。

3. 比较收到信息的 $timestamp$ 和本地信息的 $timestamp$，保存较新的路况信息。

步骤 1 保证了即使恶意节点篡改其他节点的信息进行转发，车辆在收到这些篡改数据后仍可以鉴别出消息是伪造的。因此本文考虑的恶意节点攻击方式仅为修改自己的行程时间。步骤 2 保证了不同节点发送的路况信息不会相互覆盖，也保证了同一节点多次广播的同一路况信息能够经由步骤 3 合理选取。步骤 3 利用 $timestamp$ 保证信息的实时性，让新产生的路况信息能够覆盖原信息。

3.4 道路信息投票流程

在本地的路况信息数据库 M_{recv} 中会保存恶意节点发送的恶意信息，RIDTM 的目的就是尽量避免恶意数据被更新到本地地图中而影响寻路效率。因此，RIDTM 的主要内容就是在更新本地地图前，选择 M_{recv} 中合理路况信息的算法。

我们采用文献[12]中的方法，利用 D-S 理论来描述信任。首先定义信任空间 $\Omega=\{T,\overline{T}\}$。$T$ 表示对消息 M 信任，$\overline{T}$ 表示不信任。定义假设 $H=\{T\}$表示 M 可信；假设 $\overline{H}=\{\overline{T}\}$表示不可信；假设 $U=\Omega$ 表示 M 不确定是否可信。进一步定义 mass 函数：

$$\begin{aligned} &m(H)=\alpha \\ &m(\overline{H})=\beta \\ &m(U)=1-\alpha-\beta \end{aligned} \tag{2}$$

其中，$0\leqslant\alpha,\beta\leqslant1$ 且 $\alpha+\beta\leqslant1$。

其信任的合成方式为：

$$m_1(H)\oplus m_2(H)=\frac{1}{K}(m_1(H)m_2(H)+m_1(H)m_2(U)+m_1(U)m_2(H))$$

$$m_1(\overline{H})\oplus m_2(\overline{H})=\frac{1}{K}(m_1(\overline{H})m_2(\overline{H})+m_1(\overline{H})m_2(U)+m_1(U)m_2(\overline{H}))$$

$$m_1(U)\oplus m_2(U)=\frac{1}{K}m_1(U)m_2(U) \tag{3}$$

其中，

$$K=m_1(H)m_2(H)+m_1(H)m_2(U)+m_1(U)m_2(H)+m_1(\overline{H})m_2(\overline{H})+m_1(\overline{H})m_2(U)+m_1(U)m_2(\overline{H})+m_1(U)m_2(U) \tag{4}$$

采用这种定义方式，可以描述每个路况信息的可信程度，并且合成多个不同路况信息的信任评价。

假设对 M_{recv} 指定路段 l_j，共存有 n 条对应路况信息 M_j^i，我们进一步说明本地投票算法：

1. 对每一个信息 M_j^i 计算

$$T_j^i=T(M_j^i,M_j^i)\oplus T(M_j^i,M_j^i)\oplus\cdots\oplus T(M_j^i,M_j^n) \tag{5}$$

其中，$T(M_j^i,M_j^i)$ 函数的输出为一个信任评价三元组(x,y,z)，按 D-S 理论描述：$x=m(H)$表示信任度，$y=m(\overline{H})$表示非信任度，$z=m(U)$表示不确定度。多个三元组的合成方式参考式(3)和式(4)。

$T(M_j^i,M_j^i)$设计可以根据不同场景进行调节，本文给出的参考定义如下：当 $t_j^i\leqslant1.1\times t_j^i$ 且 $t_j^i\geqslant0.9\times t_j^i$，信息相似，返回(0.9,0,0.1)表示充分信任；当 $t_j^i\leqslant1.2\times t_j^i$ 且 $t_j^i\geqslant0.8\times t_j^i$，信息相容，返回(0.6,0,0.4)表示可信任，但不完全信任；当 t_j^i 不能满足前两个条件时，说明信息相斥，若 v_k 为受信车辆，返回(0.9,0,0.1)表示完全信任受信车辆，否则返回(0,0.8,0.2)表示不可信任。T 函数的设计的主要依据是现实中如果路况信息两者之间越相近，那么它们代表的道路拥堵水平就越接近，两者之间越应当给出信任的评价；若两者的区别较大，那么它们所指的道路拥堵水平相悖，因此需要给出不信任的评价。本文的设计仅为了验证投票算法的可行性，现实中，车辆行程时间可能存在波动，因此计算信任评价时可以采用线性或是指数型函数。

2. 选出 T_j^i 中 x(三元组第一个，即信任度)最大的 T_{max}。若 $T_{max}>threshold$，取 T_{max} 对应的 M_j^i 作为路况信息；否则，表明数据不确定度过大，无法给出合理解，并不更新本地地图。不确定度过大时，车辆也可以简单随机地选取一条信息作为新的道路通行时间，或是和邻居节点进行数据交换后，采集更多证据给出判断。

相比一般的投票算法，RIDTM 引入了 D-S 理论不确定度的概念。当收到恶意信息和正常信息数量相仿时，往往会形成两个集团形式的评价分布。集团内部，行程时间相仿，相互之间会产生信任评价；集团之间，行程时间相悖，容易产生不信任评价。这些相反的信任评价合成之后，会产生不确定度很大的信任评价。一般的投票算法在处理此类情况时，倾向于选择数量占优的一方，从而容易造成恶意信息因为少量的数量优势就被选取的情况。在 RIDTM 中数据有较大分歧的情形下，就会形成 T_{max} 达不到 $threshold$ 的局面，本文给出了几种可选措施，其相比一般投票更为理性。

BI 需要路况信息两者之间存在明确的相斥情形，才能给出适当的准确性评价。本文应用的 D-S 理论对相斥的描述(不可信任)保留了一定的不确定性，而且对于相斥和相似之间也定义了过渡的相容评价(不完全信任)。由于相比其他类型的证据，路况信息之间的相容特性要比相斥特性更显著，因此用 D-S 理论代替 BI 能带来更好的容错特性，在我们的仿真中也能看到其容错性高的特点。

4 仿真实验

为了验证算法的有效性，同时仿真出车载自组织网络动态寻路和消息散布的情形，我们选择文献[21]提出的仿真平台。此平台利用 sumo[22](版本为 0.12.3)仿真车辆交通，利用 NS2(版本为 2.34)仿真网络通信，两者之间利用 TraCI 协议交互。

地图文件取自 OpenStreetMap 数据库[23]，为江苏南京市中心。路段仅选择了限速在 40km/h 以上的一级和二级公路，总体覆盖了 8500 米×9500 米的区域。每辆车在仿真开始前确定了出发地和目的地，最少直线距离在 4000 米以上。车辆出发时间在 1～200 秒内均匀分布。每个路段设定的通行时间阈值为 150 秒，如果车辆在此时间内没有通过一条道路，就判断道路发生拥堵，广播此时的路况信息。仿真中车辆共 1000 辆，未装备广播设备的车辆达 600 辆。本文主要关注于攻击者数量和攻击方式，所以受信车辆固定为装备广播设备车辆的 10%，即 40 辆。统计中恶意车辆的占比指恶意车辆占装备广播设备的车辆的比例，其余车辆为一般车辆。恶意车辆的攻击方式为发送伪造路况信息，即在发送路况信息时，修改原本的行程时间为两倍或是一半。

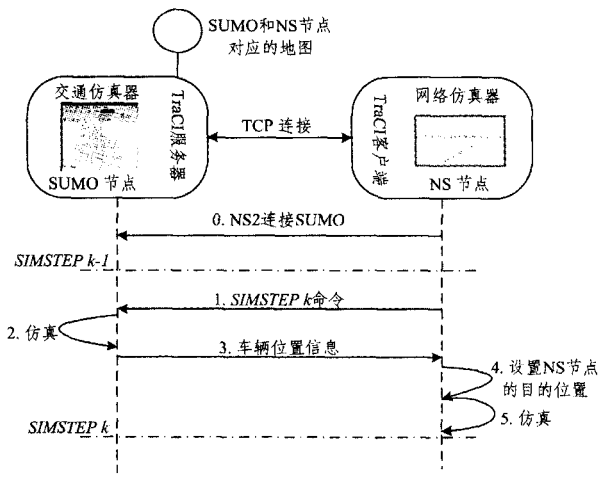

图 1 仿真环境架构

数据统计基本要素为正确、错误和不确定判断。“正确判断”指经由 RIDTM 投票判决，选择了正常信息作为道路行程时间；“错误判断”指在收到恶意信息的情况下，选择了恶意信息作为道路行程时间；“不确定判断”指由于信息分歧较大，最高信任度无法超过阈值(仿真中为 0.6)，RIDTM 只能随机选择。另外，对不确定判断进行随机选择前就形成的判断，我们称为“初步判断”；对不确定判断进行随机选择后最终获得的正确判断和错误判断称为“最终判断”。正确率、错误率和不确定率分别指正确判断、错误判断和不确定判断的占比。

4.1 算法准确率变化

RIDTM 引入不确定性后，对于全部正常但是分歧较大的数据也会做出不确定判断(Uncertainty of the Normal Data，简称 UND)。图 2 给出了各种恶意节点占比情况下 UND 在不确定判断中的占比。图 3 显示了在恶意节点夸大行程时间的攻击中，总的准确率变化情况。

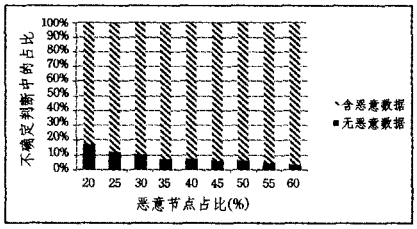

图 2　UND 占比

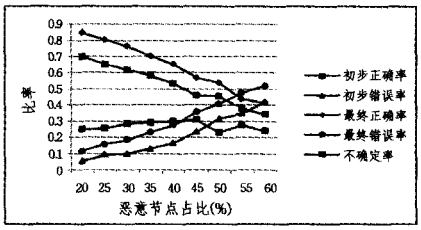

图 3　RIDTM 准确率

图 2 中，在恶意节点较少时，UND 会造成一定性能损失。而在恶意节点数量上升之后，UND 导致的性能损失对比不确定性带来的恶意识别收益并不显著。这种损失由于车辆运行环境复杂无法避免，如果采用随机选择策略，那么最终还是会选一条正常数据作为道路行程时间，实际并没有损失。

统计样本中，由于正常信息和恶意信息容易形成两个评价集团，不确定判断的比例基本在 30%左右。

由于 RIDTM 的投票特性，当恶意节点数量占少数时，初步和最终错误率都要远远低于恶意节点的占比，而最终正确率高于正常节点的占比。这得益于 RIDTM 对大部分恶意信息都给出不确定判断，同时恶意节点传播的数据并非与其数量成正比。现实中，车辆一般会优先传播受信节点的信息，因此对恶意数据有很强的抑制。随着恶意车辆占比的上升，当恶意节点数量占优时，算法性能明显下降。由于 RIDTM 仅作为恶意信息鉴别算法，无法从源头上抑制恶意信息的产生，因此错误率的上升难以被抑制。

4.2　不同攻击方式对比

由于 RIDTM 算法采用信任投票的判决形式，因此算法面对恶意节点夸大或减少行程时间的攻击都能有效运作。我们选择了比较有代表性的 2 倍时间和 0.5 倍时间作为比较标准，一些小的幅度更改实际并不能视为有效攻击，而更大的幅度更改并不能进一步影响算法的正确率。图 4 对比了两种情况下算法的正确率。两者相差最大为 5.8%，平均相差为 3.4%，可见算法的有效性并不随着攻击形式的变更产生变化，影响算法有效性的主要因素是受信节点和恶意节点的占比。

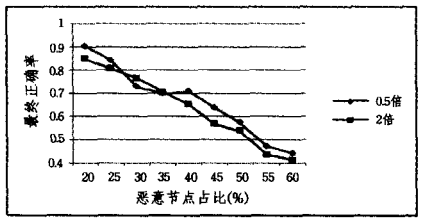

图 4　算法针对不同攻击方式的正确率

4.3　算法对比

为了更好评价 RIDTM，引入对比算法：理想投票算法和原始算法。理想投票算法指车辆预知信息的善恶情况，选择善恶信息中数量较多的一方，若数量一致，选择道路时间最大的信息。这种算法提前预知了信息的善恶情况，并基于数量做出判断，因此称为理想投票算法。原始算法指车辆选择行程时间最大的路况信息，这种算法是一般寻路算法中常用的模式。两类算法的正确率和错误率都是利用 RIDTM 完全相同的路况信息得到的。

图 5 和图 6 分别给出了它们在恶意节点夸大行程时间的攻击中的正确率对比和错误率对比。

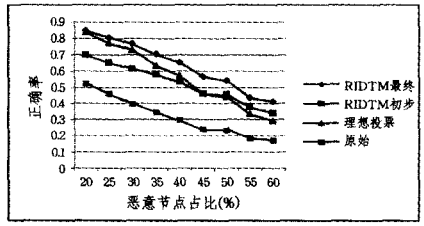

图 5　算法正确率对比

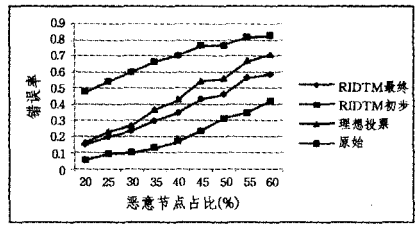

图 6　算法错误率对比

由于不确定性会造成正确率的下降，在恶意节点较少的情况下，RIDTM 的初步正确率不及理想投票算法，但是在随机选择后的最终正确率最高，说明 RIDTM 实际找寻正常信息的能力要高于另外两种算法。随着恶意节点的上升，在恶意节点超过 50%时，对比算法的正确率都低于正常节点的占比，而 RIDTM 中随着 UND 数量的下降，正确率基本保持与正常节点一致，略好于对比算法。这说明在恶意节点数量较多的环境下，RIDTM 的鲁棒性要优于对比算法。

原始算法的错误率代表了最差情况，理想投票的错误率接近甚至高于恶意节点占比，改善有限。由于 RIDTM 中不确定判断涵盖了很多恶意数据，在恶意节点较少时，直接给出错误判断的概率（初步错误率）在 20%以下，比理想投票算法降低 10%以上；在恶意节点数量上升到 50%以上时，初步错误率才有明显上升，但和理想投票算法的差值最大相差约为 30%。这得益于恶意信息的影响主要被反映到不确定率上，而不是直接形成错误判断。考虑到不确定判断还有一定概率转化为错误判断，最终错误率反映的错误概率更接近实际情况。在恶意节点较少时，最终错误率基本低于 30%，和理想投票算法近似；恶意节点变多时，错误率和理想投票算法的差距逐渐拉大，最多比理想投票算法错误率下降 10%。

4.4　到达时间比较

恶意节点修改路况信息造成的影响是造成车辆路由混乱，无法计算出合理的行程路线。在 RIDTM 引入后，一部分恶意信息被过滤掉，因而车辆能计算出足够优秀的路线（由于道路情况多变，车辆难以得到最优路线）。

在应用 RIDTM 后，并不是所有车辆的行程时间都因此改善了，统计 50%占比的恶意车辆夸大攻击中应用 RIDTM 后的车辆行程时间和之前相比的比值。若比值小于等于 1，则表示车辆的行程时间得到了改善，否则行程时间受到了延误。图 7 中 84.6%的车辆时间比小于等于 1，即大部分车辆因为 RIDTM 改善了路线。另外有 15.4%的车辆因为环境改变后造成新的拥堵而产生了新的延迟，比原先的行程时间更长。总体上来说，RIDTM 修正了大部分被恶意信息误导的错

误路线，让更多车辆能够更快到达目的地。

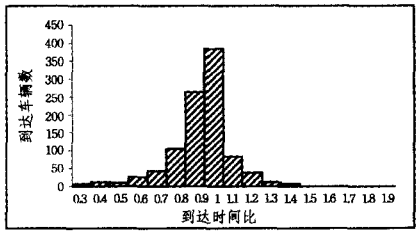

图 7　到达时间对比

结束语　本文基于真实的场景进行仿真，证明了利用基于数据的信任模型和 D-S 理论能够在存在恶意节点的环境下，不增加额外的数据交换，很好地解决了路况信息伪造问题，同时改善了车辆的行程时间。但是，当恶意节点数量超过一定比例时，基于数据的信任模型难以胜任恶意鉴别的工作，需要引入 RSU 等第三方的数据来源来提高路况信息鉴别的可靠性。另外，公交车辆路线固定，客观反映道路实际情况，作为受信车辆参与到路况信息广播中，有利于一般车辆更好地区分恶意节点。总的来说，RIDTM 算法能在车载自组织网络寻路中鉴别恶意信息、过滤异常信息，并且容易集成到已有的成熟寻路算法中，对存储空间和计算能力的要求不高，非常适用于提高常用车载自组织网络寻路算法的安全性。

参 考 文 献

[1] Nzouonta J, Rajgure N, Wang G, et al. VANET routing on city roads using real-time vehicular traffic information[J]. IEEE Transactions on Vehicular Technology, 2009, 58(7): 3609-3626

[2] Raya M, Papadimitratos P, Gligor V D, et al. On data-centric trust establishment in ephemeral ad hoc networks[C]// Proceedings of INFOCOM 2008. The 27th Conference on Computer Communications. Phoenix, USA, 2008: 1238-1246

[3] Shafer G. A mathematical theory of evidence[M]. Princeton: Princeton University Press, 1976

[4] Eschenauer L, Gligor V D, Baras J. On trust establishment in mobile ad-hoc networks[C]// Proceedings of Security Protocols. Berlin, Germany, 2004: 47-66

[5] Sun Y L, Yu W, Han Z, et al. Information theoretic framework of trust modeling and evaluation for ad hoc networks[J]. Selected Areas in Communications, 2006, 24(2): 305-317

[6] Theodorakopoulos G, Baras J S. On trust models and trust evaluation metrics for ad hoc networks[J]. Selected Areas in Communications, IEEE Journal, 2006, 24(2): 318-328

[7] Buchegger S, Le Boudec J Y. A robust reputation system for peer-to-peer and mobile ad-hoc networks[C]// Proceedings of P2PEcon. Cambridge MA, USA, 2004

[8] Ganeriwal S, Balzano L K, Srivastava M B. Reputation-based framework for high integrity sensor networks[J]. ACM Transactions on Sensor Networks (TOSN), 2008, 4(3): 15

[9] Mundinger J, Le Boudec J Y. Reputation in self-organized communication systems and beyond[C]// Proceedings of the 2006 workshop on Interdisciplinary systems approach in performance evaluation and design of computer & communications systems. Pisa, Italy, 2006: 3

[10] Zouridaki C, Mark B L, Hejmo M, et al. Robust cooperative trust establishment for MANETs[C]// Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks. Alexandria, VA, USA, 2006: 23-34

[11] Mejia M, Peña N, Muñoz J L, et al. A game theoretic trust model for on-line distributed evolution of cooperation in MANETs[J]. Journal of Network and Computer Applications, 2011, 34(1): 39-51

[12] Wu A, Ma J, Zhang S. RATE: A RSU-Aided Scheme for Data-Centric Trust Establishment in VANETs[C]// Proceedings of Wireless Communications, Networking and Mobile Computing (WiCOM). Wuhan, China, 2011: 1-6

[13] 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

[14] Jøsang A. An Algebra for Assessing Trust in Certification Chains[C]// Proceedings of NDSS. San Diego, California, USA, 1999, 99: 6

[15] Chen T M, Venkataramanan V. Dempster-shafer theory for intrusion detection in ad hoc networks[J]. Internet Computing, IEEE, 2005, 9(6): 35-41

[16] Siaterlis C, Maglaris B. Towards multisensor data fusion for DoS detection[C]// Proceedings of the 2004 ACM symposium on Applied computing. Nicosia, Cyprus, 2004: 439-446

[17] Jiang T, Baras J S. Trust Evaluation in Anarchy: A Case Study on Autonomous Networks[C]// Proceedings of INFOCOM. Barcelona, Catalunya, Spain, 2006

[18] Ostermaier B, Dotzer F, Strassberger M. Enhancing the security of local dangerwarnings in vanets-a simulative analysis of voting schemes[C]// Proceedings of Availability, Reliability and Security. Prague, Czech, 2007: 422-431

[19] Sumra I A, Ahmad I, Hasbullah H, et al. Classes of Attacks in VANET[C]// Proceedings of Electronics, Communications and Photonics Conference (SIECPC). Riyadh, Saudi Arabia, 2011: 1-5

[20] Shamir A. Identity-based cryptosystems and signature schemes[C]// Proceedings of Advances in Cryptology. Springer Berlin Heidelberg, 1985: 47-53

[21] Wegener A, Piórkowski M, Raya M, et al. TraCI: an interface for coupling road traffic and network simulators[C]// Proceedings of 11th communications and networking simulation symposium. New York, USA, 2008: 155-163

[22] Behrisch M, Bieker L, Erdmann J, et al. SUMO-Simulation of Urban MObility-an Overview[C]// Proceedings of The Third International Conference on Advances in System Simulation (SIMUL 2011). Barcelona, Spain, 2011: 55-60

[23] Haklay M, Weber P. OpenStreetMap: User-Generated Street Maps[J]. IEEE Pervasive Computing, 2008, 7(4): 12-18

(上接第 88 页)

[7] 邓绍江，李艳涛，张岱固，等. 一种基于混沌的 JPEG2000 图像加密算法[J]. 计算机科学，2009，36(5)：273-275

[8] Hong S C, Li C T, Chen H K, et al. A high speed and high security encryption scheme for JPEG2000 using a chaotic system[C]// Fuzzy Systems and Knowledge Discovery (FSKD), 2011 Eighth International Conference on. IEEE, 2011, 4: 2150-2153

[9] Stutz T, Uhl A. Complexity analysis of the Key-dependent Wavelet Packet Transform for JPEG2000 encryption[C]// 2012 19th IEEE International Conference on Image Processing (ICIP). IEEE, 2012: 2633-2636

[10] Nakachi T, Toyoshima K, Tonomura Y, et al. Layered Multicast Encryption of Motion JPEG2000 Code Streams for Flexible Access Control[J]. IEICE Transactions on Information and Systems, 2012, 95(5): 1301-1312