文章编号:1009-3087(2015)02-0129-07 DOI:10.15961/j.jsuese.2015.02.020

# 基于贝叶斯理论的VANET安全路由信任模型

吴启武,刘青子
(武警工程大学 信息工程系,陕西 西安 710086)

**摘 要**:由于车联网(VANET)节点具有高度移动性和相遇临时性,因此节点间的信任管理变得更加困难。针对此问题,利用信任分类与动态管理的方法,在基于导航预测的地理延迟路由协议(GeoDTN + Nav)的基础上,使用Beta分布描述节点的信任情况,提出一种新的基于贝叶斯理论的车联网安全路由信任模型,以实现车联网节点间的信任量化管理。该模型在提升路由安全性的同时,具有较低的时间复杂度。实验结果表明,该信任模型是有效的,且在恶意节点排除率、分组平均到达率及端到端平均时延方面取得了较好的性能。

**关键词**:车联网;贝叶斯;信任;安全路由
**中图分类号**:TP393 **文献标志码**:A

## Trusted Model of Secure Routing for VANET Based on Bayesian Theory

*WU Qiwu, LIU Qingzi*
(Dept. of Info. Eng., Armed Police Eng. Univ., Xi'an 710086, China)

**Abstract**: In order to solve the trust management problem of vehicles, a trusted model of secure routing of VANET for quantitative trust management based on Bayesian theory was proposed. In the proposed model, classified and dynamic management method of node trust was used. Meanwhile, the Beta distribution was used to describe the trust situation of the nodes based on the routing protocol framework of GeoDTN + Nav. The proposed model not only improved the security of routing, but also had the lower time complexity and good extensibility. The experimental results showed that, the trust model is effective and has good performance in the malicious nodes removal rate, the packet average arrival rate and the end-to-end average delay.

**Key words**: vehicular ad-hoc network; Bayesian; trust; secure routing

车联网(vehicular ad-hoc network, VANET)是一种特殊的移动自组织网络[1]。由于车联网的特殊性,如高度动态性、相遇临时性、持续改变的网络拓扑等,使得车辆间的信任与合作变得困难。

目前,针对车联网信任模型的研究可以分为2大类:基于消息的信任模型[3-5]和基于实体的信任模型[6-8]。其中,基于消息的信任模型的主要判断依据来源于车辆节点接收到的信息可信度本身。文献[3-5]通过对接收消息进行可靠性评估,提出了基于消息的车联网信任模型。该类模型具有通信开销较少的优点,但是没有信任度累积和更新的概念,且需要较好的网络状况保障评价的准确度,具有较大的安全隐患。基于实体的信任模型通过对节点的交互行为进行概率统计,从而得到节点信任值。由于这类模型中的信任度可以累积和更新管理,因此其具有更好的安全性能。文献[6]通过综合计算车联网中不同节点对系统中所发生事件(比如数据报转发成功率的统计)的意见,判断该节点是否可信,由于车联网中节点众多,这种模型更适合应用于小规模的网络;文献[7]在结合直接信任和邻居节点推荐信任的基础上,提出一种基于角色和事件信任等级评价的车联网信任模型,这种分类等级模型适合于大规模网络信任管理,但是节点对应角色等级表的预先确定限制了其应用的灵活性。文献[8]提出了一种基于博弈论的车联网信任模型,对节点的信任值进行博弈分析,并根据分析结果决定是否转

**收稿日期**:2014-08-07
**基金项目**:国家自然科学基金资助项目(61402529;61003250);武警工程大学基础研究资助项目(WJY201417;XJY201403)
**作者简介**:吴启武(1981—),男,讲师,博士. 研究方向:物联网;信息安全. E-mail:wuqiwu700@163.com

发消息,但是其信任管理过程复杂度较高。另外,这些信任模型均没有详细考虑如何与路由结合的问题。

为了尽可能降低信任管理的复杂度,提升车联网路由过程的安全性,作者利用信任分类与动态管理的方法,使用 Beta 分布描述当前节点的信任情况,以 GeoDTN + Nav 路由协议为应用框架,提出了一种新的基于贝叶斯理论的车联网安全路由信任模型。

## 1 相关工作

### 1.1 GeoDTN + Nav 协议

在 GeoDTN + Nav 协议[9]中,假设每一辆汽车都配有虚拟导航接口 VNI(virtual navigator interface)。VNI 是一个与底层的车辆组件交互的轻量级封装接口,其目标是发现可以传递数据包的相邻车辆,并提供格式一致的导航交互信息。VNI 的基本数据格式被定义为一个 2 元信息组 $(I,P)$,其中:$I$ 为车辆的预测路由信息,包括详细路径、目的地、车辆的运动方向等;$P$ 为车辆的运动模式遵守预测路由信息 $I$ 的概率,值为 0% 表示车辆移动是完全随机的,为 100% 则表示车辆严格按照预定模式移动。各节点广播自己的 VNI 导航信息组,且收集相邻居节点发送的导航信息组。

根据路由需要和车辆的运动方式,GeoDTN + Nav 将车辆分类分为 4 大类,并定义了不同的类型的 VNI 2 元信息组:

1)确定路线的车辆节点(记为 A 类节点):车辆严格地沿着预先设定的路线移动,如公交车和轨道交通。例如,公交车上的 VNI 将广播的 2 元组信息为(路线,100%)。

2)确定目的地的车辆节点(记为 B 类节点):车辆严格地向着预先设定的目的地移动,然而,车辆可能采取不同的路线到达目的地。例如,出租车的 VNI 将广播(目的地,100%),因为出租车的移动有确定的目的地。

3)具有导航路线/目的地的车辆节点(记为 C 类节点):车辆可根据建议路线和目的地移动。例如,按照导航系统行驶的车辆将广播(路线/目的地,$P$%)。

4)运动未知的车辆节点(记为 D 类节点):即无法获得有关导航信息的车辆节点。由于不能获得足够的路由信息,车辆可能广播(默认,0%),如果 VNI 能够估算车辆的运动方向,则可能广播(方位,$P$%)。

### 1.2 信任模型

信任管理模型自提出以来已经过多年的研究,若按信任值表示方法来分类,主要分为 3 大类[10]:基于离散值的信任模型、基于隶属度的信任模型、基于概率值的信任模型。其中,基于离散值的信任模型需借助映射函数将离散值映射为相应的信任数值,由于离散等级划分的模糊性和信任评价的不确定性,使得这种基于离散信任值的表示不够精确;基于隶属度的信任模型通常采用模糊理论和灰色理论的方法,将实体间的信任等级表述为的多个模糊子集或灰类,这类模型适合解决模糊性和不确定性问题,但是对信任的定量描述比较困难;基于概率值的信任模型将信任值定义在[1,0]区间内,在充分考虑历史交互信息的基础上,将信任的主观性和不确定性描述为概率的随机性。文中采用的贝叶斯信任模型[11]属于第 3 类,即通过一些可观察到的变量推理获取未知的概率信息,并对评估对象在网络中的地位、历史行为记录等数据进行数学推算与数据拟合,作为后续实体与该对象进行交互的指导参考。

## 2 车联网安全路由信任模型

### 2.1 基本思想

由于车联网节点数目庞大、覆盖范围广且移动模式多样,因此如果采用完全分布式的信任管理,会造成十分庞大的数据量。而且各节点按照自己的模式行驶,短时间内与相同车节点多次相遇、交互的几率也十分有限,这样会存储很多冗余的历史信息,对信任的评判也过于主观。

GeoDTN + Nav 路由协议将各车节点分类为:A、B、C、D 4 类节点。在实际情况中,车联网在城市环境中一般会部署大量路边设施单元(road-side units,RSU)。因为 RSU 位置固定,最初由网络规划者统一部署,具有较高的安全性和信息处理能力。因此,在信任管理中,授予 RSU 相应的安全管理权限,可管理其他车辆节点的信任值。确定路线的 A 类节点特指公交车和轨道交通等,由于其严格按照既定的路线和班次运行,覆盖城市大部分范围,并由统一的公共交通运输公司管理、部署、配备驾驶人员,因此其相比其他车节点具有更高的可信任性,也可以作为辅助信任管理的主体。

安全路由信任管理方案的基本思想如下:根据 GeoDTN + Nav 路由协议中车辆节点的分类,给各类车辆节点和 RSU 预设不同的信任初始值,节点间相

互监视和记录行为,作为评价节点信任值的证据。其中,RSU 和 A 类节点作为信任管理的主体,可以综合自己的检测和其他节点的反馈,对各节点的信任值进行周期性更新。当某节点信任值低于预设最低信任阈值时,该节点将被加入黑名单并排除出网络。B、C、D 类节点只能读取但不能修改其他节点的和自身的信任值,且将监视到的不同情况反馈给具有评价权限的主体节点。

### 2.2　系统模型

假设网络中各节点可以监视其邻居节点的相关通信行为,信任管理中用到的相关符号定义见表 1。

**表 1　信任模型参数定义**

**Tab. 1　Parameter definitions of trust model**

| 参数 | 定义 |
|---|---|
| $M_i$ | 节点 $i$ 的标志 |
| $A$ | 诚信行为集合 |
| $B$ | 非诚信行为集合 |
| $R_i$ | 节点 $i$ 的信任分布,定义成随机变量 |
| $C_i$ | 节点 $i$ 的评价信任值,即 $R_i$ 的数学期望 |
| $C_i^{\mathrm{Type}}$ | 类型为 Type 且节点号为 $i$ 的初始信任值 |
| $t$ | 上次更新信任值的时间戳 |
| $T$ | 信任值更新的时间周期 |
| $C_{\min}^{\mathrm{Type}}$ | 类型为 Type 的节点信任阈值 |
| $k$ | 观测记录的时间点 |
| $N_k$ | 时刻 $k$ 相遇的邻居节点集合 |
| $\alpha_i$ | 邻居节点对节点 $i$ 诚实行为的观测次数 |
| $\beta_i$ | 邻居节点对节点 $i$ 非诚实行为观测次数 |

当前节点关于信任行为记录的字段定义如表 2 所示,以黑盒形式存储于节点设备中,自身不可见。

**表 2　信任行为记录字段**

**Tab. 2　Record fields of trust behavior**

| 字段号 | 字段含义 |
|---|---|
| 1 | 节点标志 |
| 2 | 节点类型 |
| 3 | 当前信任值 |
| 4 | 上次更新信任值的时间戳 |
| 5 | 行为观测记录 $(A,N_k,k)$ 或$(B,N_k,k)$ |

表 2 中:1、2 号字段为固定字段,不可修改;3、4 号字段只能按周期 $T$ 被 RSU 或 A 类节点修改;5 号字段为与当前节点相遇的邻居节点集合 $N_k$ 对当前节点行为的观测记录,集合中的邻居节点只允许在每个间隔点 $k$ 上记录观测到的当前节点行为,由 3 元组表明在何时由哪些邻居节点观测到何种行为。

车联网中节点应用贝叶斯信任评价思想,用 Beta 分布描述当前节点 $M_i$ 的信任分布,可表示为 $R_i \sim Be(\alpha_i+1,\beta_i+1)$。Beta 分布是指一组定义在(0,1)区间的连续分布,是贝叶斯理论中常用的拟合分布模型。其中,参数 $\alpha$ 和 $\beta$ 均大于零,可以通过调整 $\alpha$ 和 $\beta$ 值对由 2 种变量决定的不确定事件进行概率拟合。在信任管理中,信任度空间定义在区间[0,1]内,$\alpha$ 和 $\beta$ 定义为与评价对象正常行为和异常行为相关联的变量,其符合 Beta 分布的基本条件,可以进行拟合。

信任分布 $R_i$ 服从参数为 $\alpha$ 和 $\beta$ 的 Beta 分布,记为 $R_i \sim Be(\alpha,\beta)$。Beta 分布的概率密度函数为:

$$f(r_i;\alpha,\beta)=\frac{1}{B(\alpha,\beta)}r_i^{\alpha-1}(1-r_i)^{\beta-1} \tag{1}$$

式中,$r_i \in (0,1)$,$a>0$,$\beta>0$。

当 $a<1$ 时,$r_i \neq 0$;当 $\beta<1$ 时,$r_i \neq 1$。其概率密度函数的期望值可表示为:

$$\mu=E(R_i)=\frac{\alpha}{\alpha+\beta} \tag{2}$$

则由式(2)可得当前节点 $M_i$ 的评价信任值为:

$$C_i=\frac{\alpha_i+1}{\alpha_i+\beta+2} \tag{3}$$

信任值的更新则利用原有信任值加上新的信任评价值得到,即:

$$C_i=C_i+C_{i+1} \tag{4}$$

同时更新时间戳,并将 $C_{i+1}$ 与 $C_{\min}^{\mathrm{Type}}$ 作比较,如果小于阈值,则将该节点加入黑名单并排除出网络。

### 2.3　节点信任值初始化

当节点入网时,根据其类型设定其初值等,首次信任值初始化为 $(C_i,T)=(C_i^{\mathrm{Type}},0)$。

### 2.4　行为监测与结果汇总

由于每个节点通过 VNI 周期性地广播 2 元导航信息,因此在 GeoDTN + Nav 协议中将2 元信息扩充为$(I,P,M_i,T,L)$,其中,$M_i$ 为区别于其他节点的唯一标志,$T$ 为时间戳,$L$ 为 $M_i$ 的当前位置。在监测邻居节点的行为中,需要解决如何区分行为诚实与否的问题。在自组织网络中,判断节点诚实与否的一般方法如下:各节点转发时将数据包缓存一段时间,同时监听下 1 跳节点发出的数据包是否与自身缓存的一致,以此判断下 1 跳节点行为是否诚实。但是,车联网中如何监听下 1 跳节点发出的数据包是比较困难的,尤其在 GeoDTN + Nav 协议中,下 1 跳节点转发数据包时,上一个节点很可能已经不在能够监听的范围内。因此针对车联网和 GeoDTN +

Nav 路由协议的特点,定义以下常见的不诚实行为,为信任管理提供相关判别准则:

1) 查看当前节点位置信息 $L$,若其位置超出监测节点邻居可达范围,则有可能是伪造的位置信息或虫洞攻击;

2) 查看节点 $I$ 字段,若其没有按照预定路线行进,则有可能被攻击或捕获;

3) 查看时间戳 $T$,若导航信息长时间没有更新,则其有可能正在进行重放攻击;

4) 节点 $M_1$ 转发时,抽取数据包部分信息利用自己的私钥进行签名,附加到数据包后一同发送,后续的第 2 跳节点 $M_3$ 用 $M_1$ 的公钥对附加数据包解密,对比原数据包,若一致则证明上 1 跳节点 $M_2$ 没有恶意篡改,否则认为上 1 跳节点篡改了数据包内容;

5) 节点 $M_1$ 通过节点 $M_2$ 转发数据包给节点 $M_3$,采用2 跳 ACK 确认回传机制,在回传时间门限 $T$ 内,只有节点 $M_1$ 收到节点 $M_2$ 和 $M_3$ 2 跳节点的确认信息,才认为节点 $M_2$ 没有出现异常行为,否则认为 $M_2$ 可能发起了黑洞或灰洞攻击。

由于如何判定节点的不诚实行为十分复杂且具有主观性,因此在具体应用中,该模型允许管理员可以根据具体情况增加新的判别准则。

例如,图 1 中各节点广播虚拟导航接口 VNI 信息,车 A 与车 B 可收到对方广播信息,互为邻居节点,则 A 与 B 互相监视行为,到时隙间隔点 $k$ 时,对对方的行为进行记录,写入相应字段。

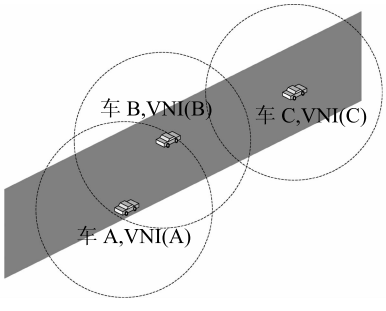


**图 1 节点 A 和 B 相互监测行为**

**Fig. 1 Mutual surveillance of node A and B**

## 2.5 信任值更新

若当前节点 $M_i$ 与 RSU 或 A 类节点相遇时,则进行信任值更新,具体步骤如下:

1) RSU 或 A 类节点查看当前节点中的 $T$ 字段,若时间不满一个周期则暂时不对其进行更新,否则进行步骤 2)。

2) RSU 或 A 类节点查看当前节点中的 5 号字段,统计 $\alpha_i$ 和 $\beta_i$。再用式(4)对节点 $M_i$ 的信任值进行更新,并加上时间戳 $T$,更新为新的 $(C_i, T)$。

关于 $\alpha_i$ 和 $\beta_i$ 的统计,RSU 或 A 类节点需要对各记录进行两两比较,排除对同一行为的重复记录,具体规则如表 3 所示。首先将记录按照诚实和不诚实分为 2 类,再按照表 3 的规则,在 2 类数据中分别统计诚实和不诚实行为的次数。

**表 3 行为统计规则**

**Tab. 3 Behavior statistic rules**

| $i_x == i_y$ | $j_x == j_y$ | $k_x == k_y$ | 1 次 | 2 次 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 |

表 3 中:$i$ 为被评价的节点,$j$ 为进行评价的邻居节点,$k$ 为评价的时刻,$x$ 和 $y$ 分别为不同的记录;$i_x == i_y$ 用来判断 2 条记录是否为被评价节点的同一行为,$j_x == j_y$ 用来判断 2 条记录是否为相同的邻居节点产生,$k_x == k_y$ 用来判断 2 条记录是否为相同的时刻产生,共 3 个判断条件、8 种状态;1 表示此记录满足相关判断条件成立,0 表示此记录不满足相关判断条件;1 次、2 次均表示满足相应条件下行为被记录的次数,其中同一节点同一时刻的行为只允许被记录一次。

3) RSU 或 A 类节点比较 $C_i$ 和 $C_{\min}^{\text{Type}}$,当前者大于后者时,不采取任何行动,否则将 $M_i$ 加入黑名单并广播节点 $M_i$ 为不可信节点,其他收到该信息的节点继续广播。所有接到该广播的节点此后都拒绝为节点 $M_i$ 服务,将其排除出网络。

例如,图 2 中,车 C 与 RSU 相遇,RSU 则可以更新节点 C 的信任值。

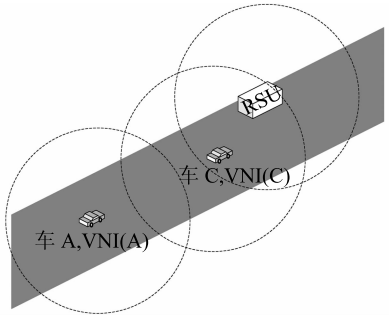


**图 2 RSU 更新节点 C 的信任值**

**Fig. 2 Updated trust value of RSU to C**

RSU 先查看节点 C 上次更新的时间戳,发现更新时间已经超过一周期,则汇总周期中其他节点对节点 C 行为的记录,计算出节点 C 的信任值,RSU 查看节点 C 的类型,将其信任值与该类型信任值最小阈值作比较,若小于阈值,则将节点 C 加入黑名单,广播黑名单信息。否则,则将新的信任值写入相应字段。

### 2.6　信任退化因子

由于随着时间的推移,信任可能会逐步降低,因此需要在各节点中引入信任退化因子 $\lambda(t)$,$\lambda(t)$ 是参数为时间 $t$ 的函数,引入退化因子的初始时刻从每一次信任值更新后开始,直至下一次更新结束。引入信任退化因子的好处是可以防止恶意节点故意躲避与 RSU 或 A 类节点的相遇,避免信任值的更新。信任退化因子定义如下:

$$\lambda(t) = k \times t \tag{5}$$

式中,$t \in (0,T)$,$k > 0$。

引入退化因子后,节点的信任值 $C_i$ 为一个随时间平滑缓慢递减的函数,且当 $C_i$ 随着时间的推移而逐步逼近 $C_{\min}^{\text{Type}}$ 后,$\lambda(t)$ 将被置为0,使节点不因为长时间没有更新信任值而使 $C_i$ 低于 $C_{\min}^{\text{Type}}$,即:

$$C_i = \begin{cases} C_i - \lambda(t), C_i > C_{\min}^{\text{Type}}, t \in T; \\ C_{\min}^{\text{Type}}, C_i = C_{\min}^{\text{Type}}; \\ C_i, C_i < C_{\min}^{\text{Type}} \end{cases} \tag{6}$$

退化因子的引入符合信任“慢增快降”的特性,可以更好地反映出节点间交互的信任关系。

## 3　信任模型分析与实验评估

### 3.1　模型分析

**定理 1**　单个时间周期内,基于贝叶斯理论的车联网安全路由信任模型的时间复杂度至多为 $O(\tau \times n)$,其中,$\tau$ 为单个时间周期所划分的时隙数目,$n$ 为单个时间周期内与目标节点相遇的节点数量。

证明:在单个时间周期内,车联网安全路由信任管理模型中,其初始化时间为 $O(n)$;行为监测时由 $n$ 个相遇节点在 $\tau$ 个时隙上对目标节点进行行为记录,所需要的时间为 $O(\tau \times n)$;信任值更新每个周期至多一次,比较各记录排除重复记录,需要遍历各记录3遍,因此时间复杂度为 $O(\tau \times n)$;利用记录的行为次数计算信任值,时间复杂度为 $O(\tau \times n)$。综上,车联网安全路由信任管理模型的时间复杂度至多为 $O(\tau \times n)$。

**定理 2**　基于贝叶斯理论的车联网安全路由信任模型可提升路由的安全性和扩展性。

证明:基于贝叶斯理论的车联网安全路由信任模型属于概率信任模型,相比于现有的基于离散值的信任模型和基于隶属度的信任模型,提出的模型在充分考虑历史交互信息的基础上,能将信任的主观性和不确定性描述为概率的随机性,克服了基于离散值的信任模型中信任值表示不够精确的问题,同时避免了基于隶属度的信任模型存在的对信任的定量描述困难的问题。通过在 GeoDTN + Nav 路由协议中引入信任管理机制,可以动态评判节点的可信程度,掌握节点行为动向,可实现对节点行为的有效监管。信任管理机制可以监测内部恶意节点的攻击,如伪造的位置信息、重放攻击、篡改攻击等,再通过广播黑名单,将不可信节点排除出网络。因此,该模型的引入提高了原有路由协议的安全性。提出的模型明确了信任管理的主体,同时解决了分布式系统中信任值管理和存放不同步的问题。对于不诚实行为的判定定义了相关规则,实际应用时允许管理员根据实际情况定义更多的类型,并可以随时间更新。此外,新节点加入网络时,运营商给其分配了合法身份、定义了相应的初始信任值,其他节点无需更新任何信息,只需在相遇时读取信任数据即可,因此具有良好的可扩展性。

### 3.2　实验评估

#### 3.2.1　实验设置

以 VanetMobiSim + NS2 作为仿真工具,采用其中的 VanetMobiSim[12] 生成道路拓扑结构和生成车辆移动模型,即先使用 VanetMobisim 生成车联网轨迹文件,然后将这些轨迹文件直接导入到 NS2[13] 中进行仿真。实验有关参数设置如表 4 所示。

**表 4　实验参数**

**Tab. 4　Experimental parameters**

| 参数 | 设定值 |
|---|---|
| 道路拓扑 | 城市道路 |
| 移动模型 | 智能驾驶者模型 |
| 路由协议 | GeoDTN + Nav 或改进版本 |
| 分组类型 | 恒定比特率 |
| 分组大小/Byte | 512 |
| 节点数目 | 20 ~ 100 |
| 节点类型 | RSU、A 类、B 类、C 类、D 类 |
| 恶意行为 | 伪造、重放、篡改和丢弃分组 |
| 仿真区域/(m × m) | 1 500 × 1 500 |
| 仿真时间/s | 200 |

3.2.2 实验结果与分析

从恶意节点排除率、分组平均到达率和端到端平均时延3方面,来测量所提出模型的性能。

1)恶意节点排除率

实验设定恶意节点的比例为4%且仅存在于B、C和D类节点中,RSU和A类节点为信任管理主体节点,运行改进后的GeoDTN+Nav路由协议。实验结果如图3所示。

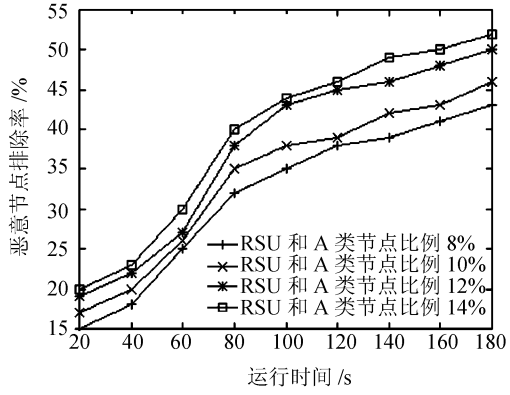


图3 不同信任主体比例的恶意节点排除率

**Fig. 3 Removal rate of malicious nodes of different trust body rates**

由图3可知,随着运行时间的增加,恶意节点排除的概率随之增大。这是由于随着车辆之间的移动,B、C和D类节点与RSU和A类节点的相遇概率增大,即节点的综合信任评价值更新次数增多,对于低于信任阈值的恶意节点,通过提出的信任模型的黑名单广播机制将其排除出网络。另外,随着RSU和A类节点比例的增大,恶意节点排除的概率也随之增大,当信任管理主体比例达到14%且运行时间大小160 s时,恶意节点排除率达到了50%以上。

通过将基于离散值和基于隶属度的信任策略分别扩展到GeoDTN+Nav路由协议中,比较分析了这2种信任模型与提出的路由信任模型的恶意节点排除性能。实验设定RSU和A类节点比例为14%。结果如图4所示。

为了方便起见,这里将离散值信任模型记为M1,隶属度信任模型记为M2,提出的信任模型记为M3。由图4可知,与M1和M2相比,提出的模型取得了更好的恶意节点排除性能。与基于离散值的信任模型相比,在恶意节点排除率方面,基于隶属度的信任模型更适合用于GeoDTN+Nav路由协议,因此,在下面的分组平均到达率、平均时延测量中,选择基于隶属度的信任模型(M2)与提出的信任模型进行比较分析。

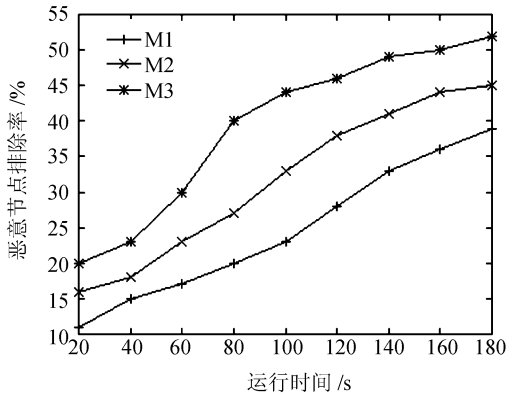


图4 不同信任模型的恶意节点排除率

**Fig. 4 Removal rate of malicious nodes of different trust models**

2)分组平均到达率

分别运行原GeoDTN+Nav路由协议、采用提出的信任模型的路由协议(记为T-GeoDTN+Nav)和采用M2模型的路由协议(记为M2-GeoDTN+Nav),变化恶意节点比例,观察分组到达率情况。实验结果如图5所示。由图5可知,与原协议GeoDTN+Nav和M2-GeoDTN+Nav相比,应用提出的信任模型的GeoDTN+Nav路由协议取得了更好的分组平均到达率。这是由于当恶意节点存在时,恶意节点可能伪造、重放、篡改和丢弃路由及分组信息,严重影响网络的性能,由于M2-GeoDTN+Nav存在对信任定量描述的困难性,因此,T-GeoDTN+Nav路由协议采用了更精确的策略选择信任值高的节点转发。

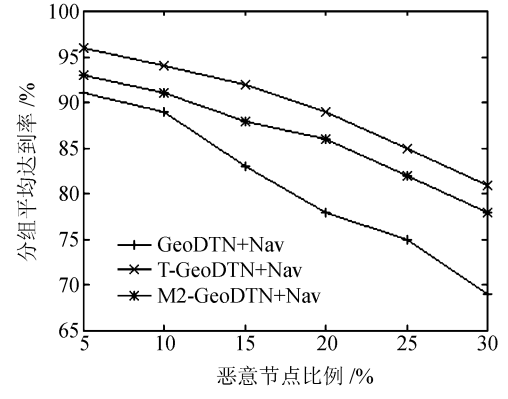


图5 分组平均到达率

**Fig. 5 Average arrival rate of packets**

3)端到端平均时延

同样,分别运行GeoDTN+Nav、T-GeoDTN+Nav和M2-GeoDTN+Nav,变化恶意节点比例,观察端到端平均时延情况。实验结果如图6所示。由图6可知,当恶意节点很少时,T-GeoDTN+Nav和M2-GeoDTN+Nav引起的端到端平均时延均略高于

原协议。当恶意节点增多时,采用 3 种不同信任模型的路由协议的时延都在增加,但是由于提出的信任模型能够尽量避开恶意节点的干扰和影响,因此,其时延最小。

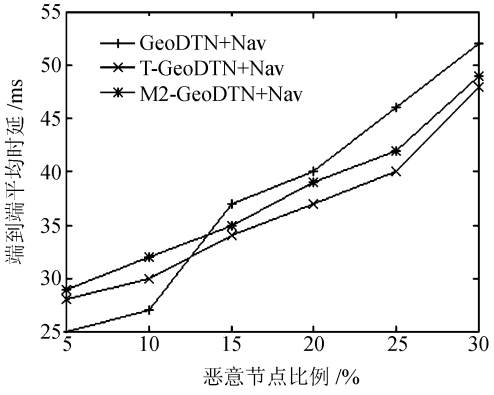


**图 6　端到端平均时延**

**Fig. 6　Average delay of end to end**

## 4　结　论

车联网作为一种新型的无线自组织网络形式,在智能交通领域具有很好的应用前景和研究价值。针对车联网的信任合作问题,在基于导航预测的地理延迟路由协议(GeoDTN + Nav)的基础上,提出一种新的基于贝叶斯理论的车联网安全路由信任模型。该模型在提升路由安全性的同时,在单个时间周期内,其时间复杂度至多为 $O(\tau \times n)$。实验结果表明,提出的信任模型是有效的,且在恶意节点排除率、分组平均到达率及端到端平均时延方面取得了较好的性能。提出的信任模型是以 GeoDTN + Nav 路由协议为框架提出的,其分类管理机制可以进一步扩展和推广到其他路由协议。因此,下一步的研究将考虑如何将该信任模型思想扩展至不同车联网路由协议中。

**参考文献:**

[1] Liu Hui, Li Hui. A Scalable anonymous authentication protocol for VANET[J]. Journal of Sichuan University: Engineering Science Edition, 2012, 44(3): 131 – 136. [刘辉,李晖. 一个易扩展的匿名车载网信息鉴别方案[J]. 四川大学学报:工程科学版, 2012, 44(3): 131 – 136.]

[2] Raya M, Papadimitratos P, Hubaux J P. Securing vehicular communications [J]. IEEE Wireless Communications, 2006, 13(5): 8 – 15.

[3] Li Q, Malip A, Marin K, et al. A reputation-based announcement scheme for VANETs[J]. IEEE Transactions on Vehicular Technology, 2012, 61(9): 4095 – 4108.

[4] Chen Liqun, Lit Q, Martin K M, et al. A privacy-aware reputation-based announcement scheme for VANETs [C]//Proceedings of 2013 IEEE 5th International Symposium on Wireless Vehicular Communications (WiVeC). Dresden: IEEE, 2013: 1 – 5.

[5] Wang Jian, Liu Yanheng, Jiao Yu. Model for trust propagation in VANETs[J]. Journal of Beijing University of Posts and Telecommunications, 2009, 32(Sup): 62 – 65. [王健,刘衍珩,焦玉. VANETs 信任传播建模[J]. 北京邮电大学学报, 2009, 32(增刊): 62 – 65.]

[6] Dotzer F, Fischer L, Magiera P. VARS: A vehicle ad-hoc network reputation system[C]//Proceedings of the Sixth IEEE International Symposium on World of Wireless Mobile and Multimedia Networks, 2005. Taormina: IEEE, 2005: 454 – 456.

[7] Ni Yan. Trust model based on graded evaluation in VANET[J]. Communications Technology, 2012, 45(11): 26 – 31. [倪妍. 基于等级评价的 VANET 信任模型[J]. 通信技术, 2012, 45(11): 26 – 31.]

[8] Liao Liefa, Sun Wei, Liu Chaoyang, et al. A trust model based on game theory in VANET[J]. Computer Measurement and Control, 2014, 22(4): 1250 – 1253. [廖列法,孙玮,刘朝阳,等. VANET 中基于博弈论的信任模型[J]. 计算机测量与控制, 2014, 22(4): 1250 – 1253.]

[9] Cheng Peichun, Lee K C, Gerla M, et al. GeoDTN + Nav: Geographic DTN routing with navigator prediction for urban vehicular environments[J]. Mobile Networks and Applications, 2010, 15(1): 61 – 82.

[10] Tian Junfeng, Cai Hongyun. Actuality and development of trust model[J]. Journal of Hebei University: Natural Science Edition, 2011, 31(5): 555 – 560. [田俊峰,蔡红云. 信任模型现状及进展[J]. 河北大学学报:自然科学版, 2011, 31(5): 555 – 560.]

[11] Nielsen M, Krukow K, Sassone V. A Bayesian model for event-based trust [J]. Electronic Notes on Theoretical Computer Science, 2007, 172: 499 – 521.

[12] Harri J, Fiore M. Vanet_mobisim_manual [EB/OL]. (2003 – 2 – 1)[2014 – 8 – 6]. http://vanet.eurecom.fr.

[13] Helmy A. UC Berkeley: Network simulator-2 [EB/OL]. (2000 – 1 – 1)[2014 – 8 – 6]. http://www.isi.edu/nsnam/ns.

(编辑　赵　婧)