

车联网中基于簇结构的可信异构路由策略研究

樊 娜, 赵祥模, 段宗涛, 王青龙

(长安大学信息工程学院, 陕西 西安 710064)

摘 要: 分析了车联网的网络结构特点, 提出了一种基于簇结构的可信路由机制, 适用于开放、异构的网络环境, 将车联网内的路由问题转化为多个中心节点间的路由路径以及目的节点所在簇内路由, 中心节点之间通过 proactive 的方式维护多条路径。仿真实验结果表明, 与传统路由方法相比, 此方法有效提高了车联网中数据传输的安全性, 降低了数据在长距离传输的时间开销, 同时提高了数据包的传输成功率。

关键词: 车联网; 可信安全; 簇; 异构路由

中图分类号: U491

文献标识码: A

文章编号: 1000-7180(2015)03-0031-05

Research on Creditable and Heterogeneous Router Strategy Based on Cluster for the Internet of Vehicles

FAN Na, ZHAO Xiang-mo, DUAN Zong-tao, WANG Qing-long

(College of Information Engineering, Chang'an University, Xi'an 710064, China)

Abstract: This paper analyzes the characteristics of the Vehicular Ad Hoc Networks, and proposes a creditable routing mechanism based on cluster structure. This method is suitable to the open and heterogeneous network environment. It changes the problem of routing in the Vehicular Ad Hoc Networks to routing in multiple central node and the routing in the cluster which the destination node is located in. multiple routing paths in center node are maintained by the method of proactive ways. Simulation results show that compared with traditional routing methods, the proposed method effectively improves the security of network data transmission, reduce the time cost of long-distance data transmission, and improve the success rate of packet transmission.

Key words: Vehicular Ad Hoc Networks; creditable security; cluster; heterogeneous router

1 引言

近年来,随着物联网相关技术在交通领域的广泛应用以及汽车工业的高速发展,车联网应运而生。车联网(Vehicular Ad Hoc Networks, VANET)通过车辆对车辆、车辆对交通基础设施的相互通信构成统一的无线通信网络。VANET 的网络部署为车辆提供了相互通信的能力,在城市交通的智能化方面起到了巨大的作用。然而,由于车联网的网络结构特点,其自身存在诸多的信息安全漏洞和隐患^[1]。

目前,已有研究人员关注车联网中通信安全和

隐私保护问题。提出了基于 PKI 的假名机制,该方法虽然在一定程度上实现对车辆网中节点的隐私保护,但是管理大量假名信息非常困难。后来,有研究人员提出基于身份签名技术的群签名技术,有效地保障了车辆隐私实现了通信安全,同时避免了管理大量假名带来的相关问题,减少了系统代价。文献[2]中提出针对 VANET 的一种条件隐私保护方案。近年来,国内相关研究人员也相继关注车联网的信息安全问题^[3-7]。

在实际应用中, VANET 还存在许多的安全问题需要解决。车联网的感知环境是开放和异构的,只

收稿日期: 2014-05-12; 修回日期: 2014-07-08

基金项目: 国家自然科学基金项目(51278058); 中国博士后科学基金(0306-110389); 交通部物联网重大专项(2012-364-208-205)

使用终端层面的隐私保护来保证终端数据隐私和安全是不完备的. 车联网中敏感的交通信息数据可能在传输过程中被恶意机构所获得, 因此在设计路由协议时必须保证路径是可信的. 提出建立符合车联网异构特点的可信路由策略模型.

2 车联网网络结构

在车联网中, 通常存在不同服务商提供部署的感知节点可互相连接, 并进行数据交换和中继, 这样构成了若干个 ad-hoc 网络. 由于终端数据隐私保护和服务安全的原因, 某些应用的数据不能经过未知或特定机构的中继节点. 如果攻击者在感知环境中部署一些中继节点, 散布虚假的拓扑信息, 宣称自己有最短路径, 那么交通信息在传输中可能被攻击者非法获取; 此外, 无线感知节点存在能量、处理能力和带宽的限制, 不会无条件转发所有数据包, 所以在感知环境中的数据路由是带有策略性的. 为了准确描述车联网中存在这类安全问题, 本文引入以下定义.

定义 1 异构策略网络 对于一个无线 ad-hoc 网络, 如果网络中节点类型、节点之间的通信距离和采用的路由协议是同构的, 但节点的路由策略却是异构的, 这样的网络被称为异构策略网络 (Heterogeneous Strategy of network). 车联网的网络结构就是典型的异构策略网络.

定义 2 路由失效 在异构策略网络通信时, 数据包在传送过程中被发送到某个中继节点, 但是该节点与数据包的具体应用不符合, 或者不被该中继节点的策略兼容, 则称之为路由失效.

通过对车联网实地测试分析, 发现存在两类路由失效的情况. 当车联网中的某个源节点要向目标节点发送数据包时, 源节点附近只有一个邻居节点, 如果该节点自身的策略不能转发来自源节点的数据包, 则出现路由失效; 当源节点周围存在多个邻居节点可以作为中间节点, 物理距离最近的邻居节点最先收到来自源节点的请求, 但如果该邻居节点自身策略不能转发, 此时也会产生路由失效.

3 基于簇结构的路由机制

3.1 逻辑簇结构的建立

为了使得数据包更容易到达目的节点, 同时减少路由开销时间, 本文提出车联网中“簇”结构的概念, 将具有平均路径短和高聚合特点的一类节点定义为簇.

本文提出的异构策略网络与普通的 ad-hoc 网络类似, 都受地理空间限制, 不具备短平均物理路径的特点. 因此在构造异构策略网中的簇结构时, 要减少节点间的逻辑跳数, 同时增加局部集聚度.

为了建立簇, 首先要选取异构策略网中转发策略较为宽松的节点, 将整个网络分为若干个簇. 簇的半径要取较小的值, 同时物理跳数也要较少, 以此保证簇的高聚合性和短平均路径, 提高路由的效率. 如果两个节点在同一团中, 本文定义其逻辑跳数为 1; 此外, 当两个节点为相邻簇的中心, 则它们的物理跳数也定义为 1. 当一个节点允许的特征越多, 其成为中心节点的可能性越大.

确定一个簇的中心节点的算法步骤如下所示.

(1) 策略更新: 对于车联网中的任意节点 N_i , 将其转发策略在网内广播 1 跳, 节点 N_i 的相邻节点将获取到 N_i 的策略. 该步骤在一个信标周期内完成.

(2) 初选候选中心节点: 在步骤 1 完成后, 网内的每个感知节点都获取了其临近点的策略, 每个节点根据获取的策略, 从中选取若干候选中心节点. 选取候选节点的计算过程为: 计算节点 N_i 的所有相邻节点的最大允许特征模板集合, 选取特征模板集合最大的 p 个节点作为候选中心节点; 该步骤在第二个信标周期完成.

(3) 更新候选中心节点: 在步骤 2 完成后, 车联网中的每个感知节点 N_i 都收到了其相邻的每个节点发来的候选中心节点集合及相应的最大特征模板集合. 感知节点对收到的若干个候选中心节点集合中的所有候选中心节点进行排序, 并比较各个最大特征模板集合的许可度, 重新选出 p 个节点 $\{O_1, O_2, \dots, O_p\}$ 作为中心节点, 并更新策略表. 计算过程如下:

① 节点 O_i 的最大特征模板数大于绝大多数 (通过实验确定合适的百分比例) 候选中心节点集合中的节点的最大特征模板.

② 节点 O_i 的相邻节点数目大于簇半径 r , 同时已经确定的中心节点数目小于 v , 以保证簇的高聚合度和短平均路径. r 和 v 的值也需要在实验中确定.

被选取的中心节点通过 proactive 共享有关的状态信息, 同时在一个信标周期内给簇内的节点发送信息, 以确定簇成员.

普通路由的优劣可以直接通过跳数进行判断, 但是在本文中定义的路由, 是带有异构转发策略, 因此还需要考虑路径的可达性. 如果某个中间节点 N_g

和目的中心节点 N_d 之间有多条路径,以兼容不同特征集的数据包,不计环路,路径数目为 p ,则定义路径 p_j 的效用函数为

$$\gamma(p_i) = \sum_{t \in T} p(t) \varphi(\text{success}(t, p_i, N_d) = \text{true}) \varphi(h) \quad (1)$$

式中, T 为最大特征空间,经过中间节点 N_g 的数据包特征模板集为 t , $p(t)$ 是特征 t 出现的概率, $\varphi(\text{success}(t, p_i, N_d))$ 是经过路径 p_j 到达目标中心节点 N_d 的概率, $\varphi(h)$ 是关于 p_j 的跳数 h 的函数, h 为路径的长度. 由于车联网自身的特点,在一定的时间范围内,网络中距离相近的节点产生和传递的数据包的特征可以聚集为有限的类别,具有连续性和相关性的特点. 因此网络中感知节点数据包特征出现的概率可以简化为距离最近的数据包特征的频率,而 $\varphi(h)$ 是路径长度的反比函数. 因此式(1)可以变换为

$$\gamma(p_i) = \frac{\sum_{t \in T} f(t, \Delta \text{time}) \varphi(\text{success}(t, p_i, N_d) = \text{true})}{\alpha h^\delta} \quad (2)$$

式中, Δtime 是时间间隔, α 和 δ 是调节因子. 当一条路径中的中间节点转发策略中特征模板集相似度较高,这条路径允许通过的数据包的类型相对越多,但是当最大特征模板集相似较高时,会对其他特征集的路径造成稀释和排挤的影响,网络中整体的可达性能会降低. 为了保障路径的可达性,对路径特征的一致性有以下要求:

$$c(p_i) > z \quad (3)$$

同时,该路径的路由转发策略还应该尽可能多的包含在最近一段时间 Δtime 范围内的数据包的特征,计算如下:

$$t \cap (\cup t(p_i)) > \lambda \quad (4)$$

通过式(3)和(4)的约束,来保障路径的整体可达性. 在满足式(3)和(4)同时,根据式(2),可以选取 q 个路径 $\{p_1, p_2, \dots, p_q\}$ 作为候选的最优路径.

3.2 基于簇结构的路由机制

通过上述步骤,将车联网划分为若干个簇,并且这些簇的中心节点之间建立了若干最短路径. 当车联网中某个节点 N_i 向目标节点 N_j 发送数据包,经过的路径由两类路径构成:跨簇路由路径(Flock Router)和簇内路由路径(Router). 跨簇路由路径完成的是将节点 N_i 的数据包发送到本簇内临近中心节点的节点属于簇内路由路径,而后由中心节点将其发送至目标节点所在簇的中心节点属于跨簇路由路径;最后目标节点所在簇的中心节点将数据包发

送给目标节点属于簇内路由路径.

跨簇路由的数据包在普通路由数据包基础上增加了与簇结构有关的字段,其中包括表示特征集允许或禁止通过的下一跳信息,跨簇时经过的中心节点等. 位于两个 hub 之间的某节点,假设收到了某个数据包,该数据包的目的节点为某 hub,首先在缓存 H 中寻找最可能的下一跳,然后转发数据包. 当每经过网络中的一个簇,就对 swttl 值减一,当其值小于零便停止跨簇的转发,因此该值是实现对路由发现区域的直径进行控制. 经过跨簇转发后,所有临近的邻居 hub 收到数据包,如果目的节点不在其所在团内,就对数据包进行继续转发,直到满足约束条件将数据包传递给目的节点.

4 实验结果及分析

为了验证本文提出的信任模型的性能,模拟车联网结构,建立了仿真实验平台,设置了与真实环境相近的场景,进行仿真实验. 实验分为两个部分:首先进行路由策略自身性能测试,取得良好效果,然后与其他路由协议进行性能对比.

在第一部分实验中,主要验证车联网内部节点密度、节点速度等因素发生变化时对本文提出的方法在路由平均时间和路由成功率指标上的影响

由于我国大部分城市市内道路都有限速规定,以西安市为例,二环内车辆最高限速为 70 km/h. 因此,在实验中设计中,车辆节点的速度最高不超过 70 km/h. 图 1 表明显示速度对路由性能的影响. 当车联网中车辆节点的平均速度为 15 km/h,整个网络中成功路由由耗费时间为 0.69 s,成功百分比为 65%;当车联网中部分节点的速度增加,平均速度为 35 km/h,整个车联网连通性提高,耗费时间减少为 0.62,且成功率提高到 72%;当车辆节点的平均速度达到 45 km/h,耗费时间减少为 0.51 s,且成功率提高到 81%;而当速度继续增加到 60 km/h,虽然网络的连通性大大加强,但是此时网络拓扑快速变化,路由路径上的节点消失的概率大大增加,耗费时间增加为 0.57,成功率快速下降为 75%;当车辆节点的平均速度继续增加达到 70 km/h,速度的增加带来的节点消失影响继续加强,耗费时间增加 0.59,成功率下降为 65%. 随着节点速度增加到一定程度,成功百分比和耗时变化趋于平缓,路由效率趋于稳定. 但考虑到在城市道路网中车辆速度由于限速要求,不会超过 70 km/h,因此簇路由的性能是可以接受的.

此外当节点的密度发生变化时,路由的效率也

会随着发生变化,图 2 所示为实验结果.其中 d1、d2、d3、d4、d5、d6 分别表示区域内节点密度值为 40、60、80、100、120、150.

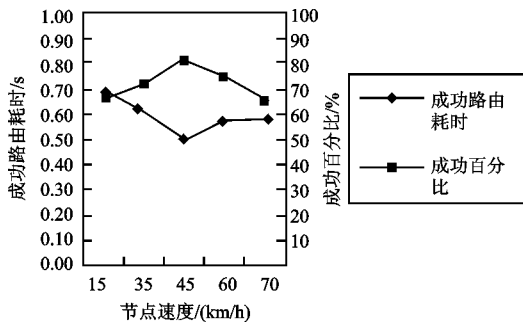


图 1 车辆节点速度对路由效率的影响

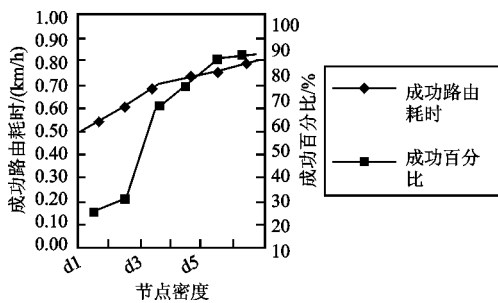


图 2 车联网节点密度对路由效率的影响

图 2 表明,当节点密度在一个某个区域范围内从 60 增加为 150 时,耗时增加了 35%,但是同时成功率提高了 6 倍左右.

第二部分实验主要对比分析本文提出的簇结构的路由的性能,引入 tagged AODV 和 AODV 两种路由机制.同时将三种路由机制在模拟车联网场景中进行实验对比.在模拟的车联网场景中分别部署了以不同速度运动的感知节点和静止的路测设备节点.路由协议参数设置为: AODV 和 tagged AODV 协议的跳数 $t_{tl}=6$ 和 $t_{tl}=10$,本文提出的协议的簇跳数 $ch=6$.

在车联网环境中,除了策略造成的路由失效外,物理路径的失效成为了严重的问题.本文实验设计了两组场景,每组场景中所有的源和目的节点的平均距离 dis 分别为 200 m 和 800 m,其他路由协议参数与低速场景一致.实验结果如图 3~6 所示.

在 $dis=200$ m 时,只需少数中继节点即可完成路由,但 AODV 协议因为存在无效路径,故成功率依然不高,tagged-AODV 协议和和本文提出的簇路由方法成功率接近,均高于 88%;但随着源目的节点距离增加,导致 AODV 协议建立的路径上路由失效的概率大大提高.相反,tagged AODV 和本文的

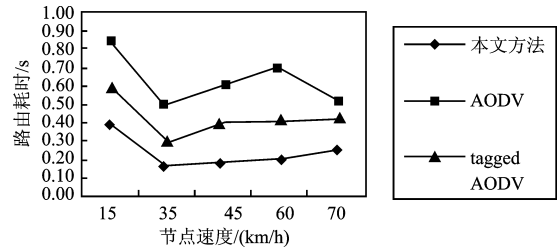


图 3 $dis=200$ m 时不同协议耗时对比

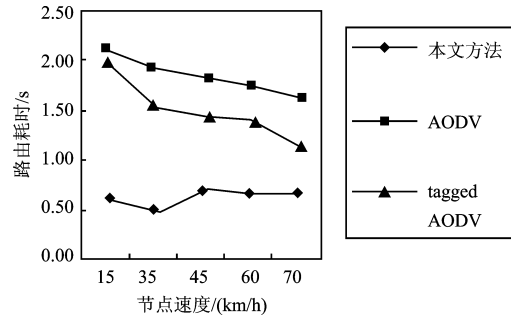


图 4 $dis=800$ m 时不同协议耗时对比

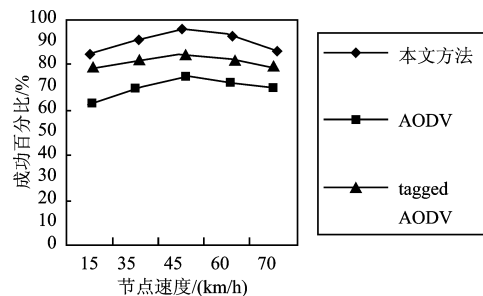


图 5 $dis=200$ m 时不同协议成功率对比

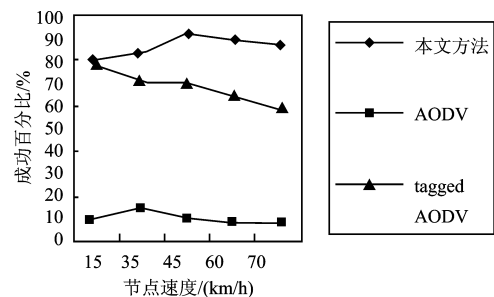


图 6 $dis=800$ m 时不同协议成功率对比

簇路由考虑了中继节点的转发策略,故有较高的成功率,尤其是本文提出的簇路由方法,成功率超过 90%,同时该方法的路由时间开销在两种场景下分别只占其他协议中效果最好的 tagged-AODV 协议的 81%、69%和 75%.

5 结束语

本文提出一种基于簇结构的转发策略,解决异

构转发策略网络中的路由安全问题,从而提高车联网中数据传输的成功率,并避免路由安全隐患。

参考文献:

- [1] Lu Rongxing, Lin Xiaodong, Zhu Haojin, et al. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications[C]// Proceedings of the IEEE INFOCOM'08. Canada: Waterloo, IEEE, 2008: 1903-1911.
- [2] 冯涛, 郭显, 马建峰, 等. MANET 节点不相交多路径安全源路由协议[J]. 计算机学报, 2009, 32(6): 1126-1133.
- [3] 陈晶, 崔国华, 洪亮, 等. 一种 Ad Hoc 网络中的安全匿名按需路由协议[J]. 计算机科学, 2007, 34(1): 29-34.
- [4] 阮星华, 徐敬东, 于博洋. VANET 中位置路由协议的安全和隐私保护[J]. 计算机工程, 2008, 34(14): 166-168.
- [5] Yang Yue, Anthony GarOn Yeh, Li Qingquan. Road network model for vehicle navigation using traffic direction approach[C]// Proceedings of SDH'08, Chi-

na, Beijing, IEEE, 2008: 613-629.

- [6] Qianhong Wu, Josep Domingo Ferrer, Ursula Gonzalez-Nicolas. Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications[J]. IEEE Transaction on Vehicular Technology, 2010, 59(2): 559-573.
- [7] Lei Zhang, Qianhong Wu, Agusti Solanas, et al. A scalable robust authentication protocol for secure vehicular communications[J]. IEEE Transaction on Vehicular Technology, 2010, 59(4): 1606-1617.

作者简介:

樊娜女, (1978-), 博士, 副教授. 研究方向为交通信息安全技术. E-mail: fnsea@chd.edu.cn

赵祥模男, (1966-), 博士, 教授. 研究方向为交通信息及控制.

段宗涛男, (1977-), 博士, 教授. 研究方向为交通信息及控制.

王青龙男, (1972-), 博士, 副教授. 研究方向为交通信息安全技术.

(上接第 30 页)

参考文献:

- [1] Bharadwaj S Amrutur, Mark A Horowitz. A replica technique for wordline and sense control in low-power SRAM's [J]. IEEE Journal of Solid-State Circuits, 1998, 33(8): 1208-1218.
- [2] Christensen D C Arandilla, Joy Alinda R Madamba. Comparison of replica bitline technique and chain delay technique as read timing control for low-power asynchronous SRAM [C]// IEEE Asia Modelling Symposium. Kuala Lumpur, 2011: 275-278.
- [3] Umut Arslan, Mark P McCartney, Mudit Bhargava, et al. Variation-tolerant SRAM sense-amplifier timing using configurable replica bitlines[C]// IEEE Custom Intergrated Circuits Conference. San Jose, CA, 2008: 415-418.
- [4] Shigenobu Komatsu, Masanao Yamaoka, Masao Morimoto, et al. A 40 nm low-power SRAM with multi-stage replica-bitline technique for reducing timing variation [C]// IEEE Custom Intergrated Circuits Conference. San Jose, CA, 2009: 701-704.
- [5] Yusuke Niki, Atsushi Kawasumi, Azuma Suzuki. A

digitized replica bitline delay technique for random-variation-tolerant timing generation of SRAM sense amplifiers [C]// IEEE Asian Solid-State Circuits Conference. Beijing, 2010: 151-154.

- [6] Yusuke Niki, Atsushi Kawasumi, Azuma Suzuki. A digitized replica bitline delay technique for random-variation-tolerant timing generation of SRAM sense amplifiers [J]. IEEE Solid-State Circuits, 2011, 46(11): 2545-2551.

- [7] JianHui Wu, JiaFeng Zhu, Yingcheng Xia, et al. A multi-stage parallel replica-bitline delay addition technique for reducing timing variation of SRAM sense amplifiers [J]. IEEE Transactions on Circuits and Systems-II: Express Briefs, 2014, 61(4): 1-5.

作者简介:

叶亚东男, (1990-), 硕士研究生. 研究方向为超大规模集成电路设计. E-mail: yeyd19900628@163.com

吴秀龙男, (1979-), 副教授, 硕士生导师. 研究方向为超大规模集成电路设计.

蔺智挺男, (1981-), 副教授, 硕士生导师. 研究方向为超大规模集成电路设计.