车用自组网节点主动通告跨层数据传输控制

李媛源[1] 宋 军[2] 金艳华[2] 黄大荣[2]
(重庆邮电大学计算机科学技术学院 重庆 400065)[1] (重庆交通大学信息科学与工程学院 重庆 400074)[2]

摘 要 为提升车用自组网中数据业务的服务质量,改进了车用无线接入技术数据传输控制机制,提出了车用自组网节点数据传输能力主动通告跨层数据传输控制方案(Active Notify EDCA,AN-EDCA)。仿真实验表明,AN-EDCA跨层数据传输控制机制有效地提升了各种应用环境中车用自组网的数据业务吞吐量,保证了车用自组网中数据业务的服务质量。

关键词 车用自组网,数据传输控制,服务质量
中图法分类号 TP393 **文献标识码** A

Cross-layer Data Transmission Control Based on Active Notify of Vehicular Ad-hoc Network Node

LI Yuan-yuan[1] SONG Jun[2] JIN Yan-hua[2] Huang Da-rong[2]
(College of Computer Science & Technology, Chonqing University of Post and Telecommunication, Chongqing 400065, China)[1]
(College of Information Science and Engineering, Chonqing Jiaotong University, Chongqing 400074, China)[2]

Abstract To enhance the QoS of data service in vehicular Ad-hoc network, we improved the data transmission control mechanism on technology of Wireless Access in Vehicular Environment(WAVE) and proposed a cross-layer data transmission control scheme based on Active Notify of vehicular Ad-hoc network node(Active Notify EDCA, AN-EDCA). Simulation results indicate, AN-EDCA cross-layer data transmission control mechanism efficiently enhances the throughput and guarantees the QoS of data service in vehicular Ad-hoc network.

Keywords Vehicular Ad-hoc network, Data transmission control, Quality of service

车用自组网(Vehicular Ad-hoc Network,VANET)以道路上行驶的车辆为主体,构建车辆间、车辆与路边固定接入点间的开放无线自组织网络,是移动自组网和传感器网络在道路交通领域的特殊表现形式[1]。与智能交通系统相结合,车用自组网可以提供交通安全预警、辅助驾驶、交通信息发布、车载电子商务和Internet接入等服务,具有广阔的应用前景。

TCP是目前广泛采用的、提供可靠端到端数据传输的网络协议,主要针对有线网络设计。在有线网络中,分组丢失主要由网络拥塞引起,TCP采用慢启动、拥塞避免、快速重传与快速恢复4种手段进行流量和拥塞控制。与有线网络相比,车用自组网具有无线信道质量差、节点高移动性、网络拓扑变化频繁、节点运动受道路限制且分布不均、信道竞争异常激烈等特点[1,5],而TCP缺乏相应的数据传输控制手段,性能受到严重制约,导致车用自组网中数据业务的服务质量恶化。因此,深入研究车用自组网中的数据传输控制机制,提升车用自组网中数据传输服务质量,具有重要理论意义和实用价值。

1 车用无线接入技术

IEEE针对车载无线通信专门制定了车用环境无线接入(Wireless Access in the Vehicular Environment,WAVE)技术标准[2],其物理层和MAC层标准为IEEE 802.11p协议,如图1所示。

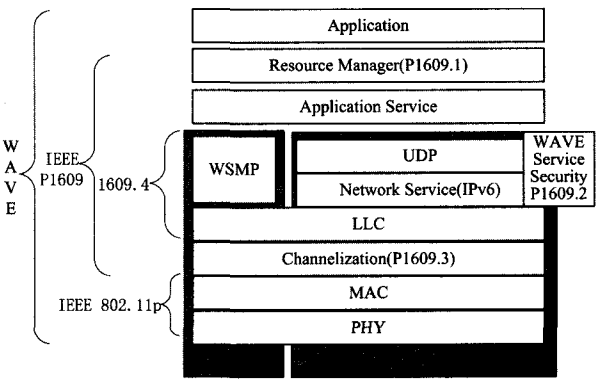

图1 WAVE体系结构

IEEE 802.11p的物理层采用IEEE 802.11a的5.8G频段和OFDM调制方式,来提高无线信道的抗干扰能力和数据传输效率;MAC层则采用IEEE 802.11e的EDCA,为各种多媒体网络应用提供QoS保障机制。

EDCA在仍然采用IEEE 802.11 DCF传输数据业务的基础上,将具有不同QoS要求的业务划分为4种接入类型(Access Category,AC),并赋予不同优先级和提供区分服务[3],如表1所列。

到稿日期:2010-07-28 返修日期:2010-10-15 本文受国家自然科学基金(61004118),重庆邮电大学自然科学基金(A2008-37)资助。
李媛源(1980—),女,硕士,工程师,主要研究方向为计算机网络与通信技术,E-mail:liyy@cqupt.edu.cn;宋 军(1971—),男,博士,教授,主要研究方向为宽带网络技术、嵌入式系统、交通信息技术。

表 1　EDCA 接入类型及其优先级

优先级	接入类型	说明
1	AC_BK	背景数据
2	AC_BK	背景数据
0	AC_BE	数据
3	AC_BE	数据
4	AC_VI	视频
5	AC_VI	视频
6	AC_VO	音频
7	AC_VO	音频

EDCA 对不同 AC 的区分服务主要通过帧间间隔 IFS、竞争窗口值 CW、内部竞争(优先级)和传输机会(Transmission Opportunity,TXOP)等参数的配置来实现,推荐参数如表 2 所列。

表 2　EDCA 默认参数配置

AC	CWmin	CWmax	AIFSN	TXOP
AC_BK	aCWmin	aCWmax	7	0
AC_BE	aCWmin	aCWmax	3	0
AC_VI	(aCWmin+1)/2−1	aCWmin	2	3.008ms
AC_VO	(aCWmin+1)/4−1	(aCWmin+1)/2−1	2	1.504ms

如图 2 所示,各种 AC 使用不同的仲裁帧间间隔(Arbitration Inter Frame Space,AIFS),AIFS[i]=SIFS+AIFSN[i]$*aSlotTime$。AIFSN[i]为 i 类 AC 在信道空闲最短帧间间隔 SIFS 后启动数据发送或退避需要等待的空闲时隙数。

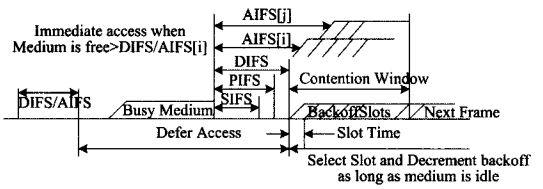

图 2　EDCA 时隙图

EDCA 为各种 AC 规定了相应的最小竞争窗口值 CW_{min} 和最大竞争窗口值 CW_{max},使各种 AC 接入信道时拥有不同的退避时间范围。

内部竞争机制在一个节点内多个 AC 同时完成退避而产生节点内数据发送冲突时,赋予高优先级 AC 信道访问权,而让低优先级 AC 继续退避。

TXOP 规定了音、视频 AC 持续占用信道的最大时长,音、视频业务可以在此时限内无需进行信道竞争而连续发送多帧,连续发送的帧之间间隔 SIFS。

2　跨层数据传输控制方案

近年来,随着无线自组网日益普及、移动自组网和车用自组网逐渐开始应用,为提高这类网络中数据业务的服务质量,研究人员分别从 TCP 协议和 MAC 协议两个方面提出了多种改进方案[1,4,5]。A2DTCP,ADTCP,I-ADTCP,TCP-Few 等 TCP 改进方案主要针对标准 TCP 协议的网络状态辨识手段不足,对伪拥塞错误地进行了拥塞控制以及 TCP 的贪婪性加重了网络负载,加剧了 MAC 层冲突,导致丢包率上升、TCP 性能和数据业务服务质量严重下降等问题,对 TCP 协议进行改进。FCR,NSAD 等 MAC 改进方案主要针对减少信道竞争冲突、节点的频繁退避和无效退避时间,提高节点数据发送公平性等问题对 MAC 机制加以改进,提高网络吞吐量和信道利用率,进而提升数据业务服务质量。

笔者在充分研究无线自组网、移动自组网和车用自组网 MAC 机制和 TCP 改进方案以及 MAC 机制对 TCP 性能的影响因素基础上,提出一种综合 MAC 机制和 TCP 协议的车用自组网节点数据传输能力主动通告跨层数据传输控制方案(Active Notify EDCA,AN-EDCA)。

2.1　基本思想

车用自组网节点密度大、运动受道路限制且分布不均,信道竞争异常激烈、冲突大,发送节点 MAC 层有效发送能力无法满足 TCP 贪婪地向网络注入的分组量,导致发送节点 MAC 层队列长期处于饱和状态,造成 TCP 报文传输经常超时,TCP 发送端频繁进入慢启动状态,吞吐量长期处于较低水平,严重影响数据业务服务质量。

TCP 协议通过拥塞窗口 cwnd 和接收窗口 rwnd 共同作用实现数据传输的流量和拥塞控制,即发送窗口 swnd=Min[cwnd,rwnd]。研究表明[6],在无线自组网和车用自组网中,当接收节点缓存大于 10 时,很少发生缓存溢出,rwnd 实际上不能准确地对 TCP 发送端实施流量控制。

AN-EDCA 跨层数据传输控制机制通过 MAC 层监测信道接入冲突率的变化(即冲突率增益)来判定发送节点 MAC 层的发送能力,并根据冲突率增益动态修改 TCP 接收端返回的 ACK 分组首部中的通告窗口值,从而动态调整 TCP 发送端的 rwnd 参数,使 rwnd 参数不仅可以反映接收端的接收能力,还能反映发送节点 MAC 层的发送能力。这样,TCP 发送端就可以根据车用自组网发送节点 MAC 层的发送能力有效地进行流量控制,提高数据业务的平均吞吐量。

2.2　算法描述

AN-EDCA 跨层数据传输控制机制的执行步骤及算法如下:

(1)信道接入冲突监测

车用自组网的信道为无线共享信道,处于载波信号覆盖范围内的所有节点不仅能够接收发送给自己的数据帧,也能接收发送给其他节点的数据帧。对于不属于本节点的数据帧直接丢弃,正确接收属于本节点的数据帧则在 SIFS 帧间间隔后发送 ACK 帧。如果信道接入产生冲突,则接收节点不会发送 ACK 帧。因此,车用自组网节点通过监测所有节点的数据帧与 ACK 帧发送过程,对整个网络的信道接入冲突进行监测。

(2)信道接入冲突率增益统计

车用自组网信道接入冲突率按式(1)计算:

$$CollRate_{avg}=CollRate[t]*\alpha+CollRate[t-1]*(1-\alpha) \tag{1}$$

式中,$CollRate[t]$为本次监测周期的信道接入冲突率,$CollRate[t-1]$为上一个监测周期的信道接入冲突率,α 为平滑因子,取值 0.85。每个监测周期的信道接入冲突率如式(2)所示:

$$CollisionRate=\frac{Collision\_num}{Total\_data\_count} \tag{2}$$

式中,$Collision\_Num$ 为监测周期内信道接入冲突的次数,$Total\_data\_count$ 为监测周期内所有车载节点发送数据帧的总数量。

车用自组网信道接入冲突率增益按式(3)计算:

$$\Delta CollRate=\frac{CollRate_{avg}[t]-CollRate_{avg}[t-1]}{CollRate_{avg}[t-1]} \quad (3)$$

(3)TCP 通告窗口动态调节

发送节点的 MAC 层在接收到 TCP 接收端返回的 ACK 分组时，根据自己所监测到的信道接入冲突率增益，对 ACK 分组首部中的通告窗口值进行动态调整：

① 当 $0<\Delta CollRate<1$ 时，表明信道接入冲突有所增加，$rwnd=rwnd * \Delta CollRate$。

② 当 $\Delta CollRate=0$ 时，表明当前信道接入冲突没有变化，$rwnd=rwnd$。

③ 当 $\Delta CollRate<0$ 时，表明当前信道接入冲突较先前有所减少，$rwnd=rwnd * (1-\Delta CollRate)$。

④ 当 $\Delta CollRate>1$ 时，表明当前信道接入冲突急剧上升，$rwnd=1$。

3 仿真与性能分析

本节利用 ns-2 对车用自组网采用标准 EDCA 和 AN-EDCA 跨层数据传输控制机制情况下的数据传输进行仿真，并分析数据业务的性能。

3.1 仿真参数设置

信道为理想信道，链路带宽为 2Mbps，物理层采用 IEEE802.11a，节点信号发射距离为 250m，MAC 层分别采用 EDCA 和 AN-EDCA 跨层数据传输控制机制，MAC 层其他参数采用 IEEE802.11e 标准值，路由协议采用 AODV，传输层采用 TCP-Reno，TCP 报文长度为 1000 Byte，应用层采用 FTP。仿真实验分别采用相对静止的单跳拓扑结构、相对移动的单跳拓扑结构、相对静止的链式拓扑结构 3 种场景，各种场景分别进行 300s 仿真实验。

3.2 性能分析

3.2.1 实验场景一：相对静止的单跳拓扑结构

仿真实验以图 3 所示的城市道路交通为场景，车载节点以 60～70km/h 的速度同向而行，即车载节点之间处于相对静止或相对低速移动状态，车载节点之间进行一对一的单跳数据传输。

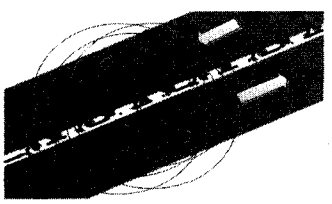

图 3 单跳拓扑结构

相对静止、单跳拓扑场景中的车用自组网数据业务吞吐量如图 4 所示。从图中可以看出，随着网络中数据业务流的数量不断增加，网络负载不断加重，数据业务的平均吞吐量呈下降趋势。AN-EDCA 根据车载节点 MAC 层数据发送能力主动控制 TCP 发送端的数据发送量，避免了因 TCP 数据发送量过大，引起车载节点信道接入冲突剧烈或 MAC 层发送缓存溢出，导致 MAC 层出现连续丢包，触发 TCP 发送端频繁进行拥塞控制和进入慢启动状态，使数据业务的吞吐量急剧下降并长时间保持较低水平。因此，AN-EDCA 跨层数据传输控制机制将相对静止、单跳拓扑环境下的车用自组网数据业务吞吐量大幅提升了约 43%。

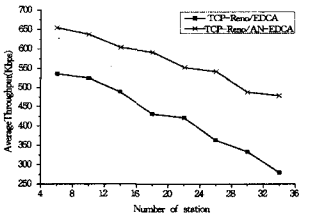

图 4 相对静止、单跳拓扑数据业务吞吐量

3.2.2 实验场景二：相对移动的单跳拓扑结构

仿真实验仍然以图 3 所示的城市道路交通为场景。在 $3000\times200m^2$ 的区域内随机分布着 50 个车载节点，以不同的速度在道路上同向或相向移动，相对移动速度分别为 5，10，15，20，25 和 30m/s，并建立 10 条数据流。

相对移动、单跳拓扑场景中的车用自组网数据业务吞吐量如图 5 所示。从图中可以看出，随着车载节点之间的相对移动速度不断增加，节点移动性成为分组丢失的主要原因，使得数据业务的平均吞吐量呈下降趋势。AN-EDCA 跨层数据传输控制机制将节点移动引起的 MAC 层丢帧通过调整节点 MAC 层发送能力参数控制 TCP 发送端的数据发送量，避免了 TCP 发送端将分组丢失错误地判断为网络拥塞而采取过激的拥塞控制并大幅降低数据发送量，导致数据业务吞吐量急剧下降。因此，AN-EDCA 跨层数据传输控制机制将相对移动、单跳拓扑环境下的车用自组网数据业务吞吐量提升了约 25%。

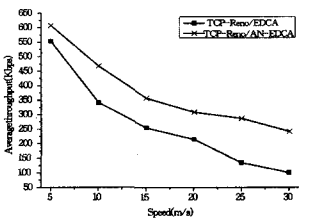

图 5 相对移动、单跳拓扑数据业务吞吐量

3.2.3 实验场景三：相对静止的链式拓扑结构

仿真实验以图 6 所示的城市道路交通为场景。车载节点以 60～70km/h 的速度同向而行，即车载节点之间处于相对静止或相对低速移动状态，相邻车载节点之间平均相隔 200m。网络中设定 5 条数据流，发送节点为 C_1-C_4，接收节点为 C_{x+n}，其中 x 取 1～4，n 为跳数，数据流传输路径长度为 2～12 跳。

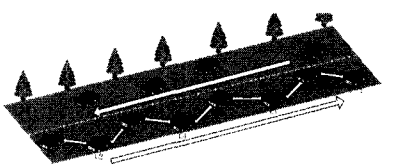

图 6 链式拓扑

相对静止、链式拓扑场景中的车用自组网数据业务的吞吐量如图 7 所示。从图中可以看出，随着传输路径跳数的增大，数据分组的传输需经过多个中间节点转发，发送冲突和分组丢失的概率增加，导致数据业务平均吞吐量呈下降趋势。当跳数超过 6 跳后，数据业务平均吞吐量基本平稳。AN-EDCA 跨层数据传输控制机制将相对静止、多跳链式拓扑环境下的车用自组网数据业务吞吐量提升了近 1 倍，但维持在 200kbps 较低水平，仅为信道容量的 10%。

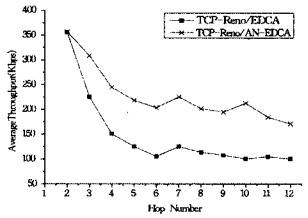

图 7　相对静止、链式拓扑数据业务吞吐量

结束语　车用自组网的固有特点严重影响了网络中数据业务的服务质量。仿真实验表明，AN-EDCA 跨层数据传输控制机制对各种应用环境中车用自组网数据业务性能均有较大提升。继续优化和改进 AN-EDCA 机制，进一步提升高速移动和多跳环境下车用自组网数据业务性能，是今后研究的重点方向。

参 考 文 献

[1] 陈立家，江昊，吴静，等. 车用自组织网络传输控制研究[J]. 软件学报，2007，18 (6)：147-149

[2] Hayashi M，Fukuzawa S，et al. Development of Vehicular Communication (WAVE) System for Safety Applications[C]// 7th International Conference on ITS. June 2007：1-5

[3] IEEE802. 11 WG，PartII：Wireless LAN Medium Access Control (MAC) and Physical (PHY) Layer Specification，Amendment 8：Medium Access Control(MAC) Quality of Service Enhancements[S]. 2005

[4] 宋军，金艳华，李媛源，等. 无线局域网 MAC 机制对 TCP 性能影响分析[J]. 计算机科学，2009，36(5)：111-114

[5] 宋军，李浩，李媛源，等. Ad-hoc 中的 TCP 改进方案—Adaptive ADTCP [J]. 计算机应用，2010，30(7)：1750-1753

[6] Fu Zheng-hua，Zerfos P，Luo Hai-yun，et al. The Impact of Multihop Wireless Channel on TCP Throughput and Loss[C]// Proc. of IEEE INFOCOM'03. April 2003

[7] 陈林，赵莉，唐亮. 网络数据传输的实现[J]. 重庆工学院学报：自然科学版，2007，21(11)：123-126

(上接第 148 页)

[3] Dolev D，Yao A C-C. On the security of public key protocols[J]. IEEE Transactions on Information Theory，1983，29 (2)：198-207

[4] Canetti R，Herzog J. Universallly composable symbolic analysis of mutual authentication and key-exchange[C]// Proc of Theory of Cryptography. LNCS 3876，2006. Berlin，Heidelberg：Springer-Verlag，2006：380-403

[5] 中国密码学会. 密码协议发展研究[R]. 2009-2010 密码学学科发展报告[D]. 北京：中国科学技术出版社，2010-04

[6] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报，2005，16 (10)：1743-1756

[7] 王圣宝，曹珍富，董晓磊. 标准模型下可证安全的身份基认证密钥协商协议[J]. 计算机学报，2007，30(10)：1842-1852

[8] Shoup V. Sequences of Games：A Tool for Taming Complexity in Security Proofs[EB/OL]. Cryptology ePrint Archive，Report 2004/332，http：//eprint. iacr. org/2004/332. pdf，2004

[9] Choudary G M，Boyd C，González N J M. Modeling key compromise impersonation attacks on group key exchange protocols[C]// Jarecki S，Tsudik G. eds. Proc. of PKC 2009. LNCS 5443，Berlin，Heidelberg：Springer-Verlag，2009：105-123

[10] 李国民，何大可. 基于身份的群密钥协商协议[J]. 计算机科学，2009，36(1)：60-64

[11] Goldreich O. Foundations of Cryptography-Basic Tools[M]. volume 1. Cambridge University Press，2001

[12] Choi K Y，Hwang J Y，Lee D H. Efficient id-based group key establishment with bilinear maps[C]// Proc. of PKC 2004，LNCS vol. 2947. Berlin：Springer-Verlag，2004：130-144

[13] 贾洪勇，卿斯汉，谷利泽，等. 通用可组合的组密钥交换协议[J]. 电子与信息学报，2009，31(7)：1571-1575

[14] Bellare M，Pointcheval D，Rogaway P. Authenticated Key Exchange Secure Against Dictionary Attacks[C]// Proc. of the Advances in Cryptology-EUROCRYPT'00. LNCS 1807. Berlin，Heidelberg：Springer-Verlag，2000：139-155

[15] Bresson E，Chevassut O，Pointcheval D，et al. Provably Authenticated Group Diffie-Hellman Key Exchange[C]// Proc. of 8th ACM CCS. New York：ACM Press，2001：255-264

[16] Bresson E，Chevassut O，Pointcheval D. Provably authenticated group Diffie-Hellman key exchange-the dynamic case[C]// Boyd C. ed. Proc. of the advance in cryptology-Asiacrypt'2001. LNCS 2248. Berlin，Heidelberg：Springer-Verlag，2001：290-309

[17] Bresson E，Chevassut O，Pointcheval D. Group Diffie-Hellman Key Exchange Secure against Dictionary Attacks[C]// Proc. of the Advances in Cryptology -ASIACRYPT'02. LNCS 2501. Heidelberg：Springer-Verlag，2002：497-514

[18] Bresson E，Manulis M，and Schwenk J. On security models and compilers for group key exchange protocols[C]// Proc. of the 2nd International Workshop on Security (IWSEC 2007). LNCS 4752. Heidelberg：Springer-Verlag，2007：292-307

[19] Bresson E，Manulis M. Malicious Participants in Group Key Exchange：Key Control and Contributiveness in the Shadow of Trust[C]// Proc. of the 4th Autonomic and Trusted Computing Conference (ATC 2007). LNCS 4610. Heidelberg：Springer-Verlag，2007：395-409

[20] Bresson E，Manulis M. Securing group key exchange against strong corruptions[C]// Proc. of ACM Symposium on Information，Computer and Communications Security (ASIACCS 2008). New York：ACM Press，2008：249-260

[21] Bellare M，Canetti R，Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols (extended abstract)[C]// Proc. of the Thirtieth Annual ACM Symposium on the Theory of Computing (STOC'98). New York：ACM Press，1998：419-428

[22] Shoup V. On formal models for secure key exchange (Version 4)[EB/OL]. RZ 3120，IBM Research，available at http：// shoup. net/，November 1999

[23] Canetti R，Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels[C]// Proc. of Advances in Cryptology-EUROCRYPT'01. LNCS 2045. Heidelberg：Springer-Verlag，2001：453-474

[24] Canetti R. Universally composable security：A new paradigm for cryptographic protocols[C]// Proc. of 42nd Annual Symposium on Foundations of Computer Science (FOCS 2001). 2001：136-145

[25] Katz J，Shin J S. Modeling insider attacks on group key-exchange protocols[C]// Proc. of the 12th ACM Conference on Computer and Communications Security (CCS'05). New York：ACM Press，2005：180-189

[26] 秦波，伍前红，王育民，等. 密钥协商协议进展[J]. 计算机科学，2008，35(9)：9-12