Overlay Token Ring Protocol for Vehicular Communication Networks

by

Jingqiu Zhang

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2007

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Jingqiu Zhang

Abstract

Vehicular communication has been an emerging topic among current wireless research. The vehicular communication can be classified to Inter-Vehicle Communication (IVC) and Road-to-Vehicle Communication (RVC). IVC and RVC support applications mainly on two aspects: safety applications aiming to reduce dangers on the road, and data applications aiming to provide information and entertainment to people on traveling. Vehicles nearby form Vehicular Ad hoc Networks (VANETs) without any fixed infrastructures. Due to the characteristics of vehicular networks such as quickly changing and unstable network topology, IVC has special requirements to the network protocols. Several MAC protocols have been appeared or improved based on previous work for IVC. But these protocols are designed either for QoS guaranteed data service or for reliable message broadcast. There is not a protocol including both application requirements and inexpensive to implement as well. MAC protocol for vehicular communication hasn't been finalized.

In this thesis, an overlay token ring protocol (OTRP) is proposed which can work on MAC layer with broadcast function and taking into the IVC features into consideration. In OTRP, vehicles are grouped to overlapped rings with a token passed in each ring as the sole right for transmission. The ring is dynamically updated in a distributed manner based on smart algorithm at each node. OTRP provides bounded delay by assigning maximum token holding time for each node. It also reduces collisions by decreasing the number of contention nodes by times of ring size. Fair and high throughput is obtained as well. Furthermore, it provides reliable and prompt broadcast of emergency messages by pre-emptively transmitting while applying the token as an acknowledgement. The time nodes reliably receive the message is within limit. Theoretical analysis is provided and simulation results are given to evaluate the performance of OTRP under saturated traffic conditions both in safety and data applications.

Acknowledgements

There are a number of people I would like to appreciate during my study and research at the University of Waterloo. First and for most, I would like to thank my supervisor Professor Xuemin (Sherman) Shen for his guidance and tremendous support in this research work. He not only shows me how to do a good academic work but also teaches me how to be a good person. It's my honor to study under his supervision.

I would like to thank my thesis reader professors Liang-liang Xie and Zhou Wang for reviewing my thesis. I would like to thank Stanley Liu for his enlightening and patient guidance during this research and thesis writing process.

I would also like to thank all the Broadband Communication Research (BBCR) lab members for their help and discussions during my study at the University of Waterloo.I would like to thank all the teachers, educators and staffs at the University of Waterloo, especially in Electrical and Computer Engineering who teach me not only the knowledge, methods and philosophy in research as well.

I would also like to thank my parents and my boyfriend for their forever supports.

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

With the increasing number of vehicles and more time spent in traveling, on-wheel mobile service has attracted great attentions both in academic and industry. Those applications include safety indication and control during driving such as obstacle warning, merging reminder, traffic accident informing, interaction between vehicles on the road such as coordination and information exchanging, entertainment and information system such as playing Internet games and booking hotels and restaurants.

However these applications require a vehicular network to provide sufficient bandwidth and reliable service. Since the vehicular networks extend to thousands of miles with merging and splitting, building enough infrastructures to cover all the road area for IVC is impractical. Therefore, the Vehicular Ad-hoc Networks (VANETs) are recommended as the de facto mode for IVC as the self-configured way for vehicles to communicate with nearby peer. Different from the traditional wireless environment, vehicular network topology is changing at a very fast speed by the vehicle's nature that challenges the protocol design.

For a fixed physical layer, VANETs require MAC layer adaptive to the volatility of vehicular networks which can achieve good fairness, high throughput for data applications and, reliable and prompt transmission for safety applications. Current Mobile Ad-hoc Networks (MANETs) supportive protocols are inadequate to deal with IVC's problems. For instance, although IEEE 802.11 standards [8] are mature in both research and implementation, it is exposed to unfairness and low throughput in ad hoc networks and no reliable broadcast is specified. The GSM/CDMA mobile cell phone system has large coverage but the bandwidth is tight for extra vehicular applications. In Europe, a TDMA-based protocol called Reliable Reserved-ALOHA (RR-ALOHA) is proposed for VANETs to provide reliable broadcast to vehicles on road which can solve hidden and exposed terminal problems [1]. However the protocol needs fully research in efficiently utilizing bandwidth and other issues such as accurate synchronization. Directional-antenna MAC is deemed to be an effective way in reducing collisions by space reuse, however this is an uneconomical way for cost consideration.

IEEE 802.11 group is standardizing 802.11p especially for both IVC and RVC. IEEE 802.11p works on the same core mechanism CSMA/CA but takes into account the safety application requirements. It applies multi-channel structure of Dedicated Short Range Communication (DSRC) with control and safety application related message in control channel for priority consideration and

six service channels for data transmission. Enhanced Distributed Control Access (EDCA) in 802.11e is used to provide different priorities to six service channels. By mapping different classes of traffic to different data channels that with pre-assigned parameters, different priorities are achieved. 802.11p is a promising MAC protocol that will be finalized in April 2009.

The token ring standards IEEE 802.4 was first implemented in wired networks by passing a token as the right to transmit. In wireless networks, wireless token ring protocol (WTRP) was proposed in [7] as one part of the PATH project in the University of California, Berkley, United States. WTRP is devised for Intelligent Transportation System for guaranteeing QoS in wireless environment and can recover from multiple transmission failures. But it can'T be implemented to a large number of nodes and is not suitable in high mobile environments. Reliable Neighbour-cast Protocol (RNP) [4] is designed to provide reliable MAC broadcast within a vehicle's neighbouring group. The neighbouring group is decided by a distributed voting scheme. Due to the voting scheme as well as aggressive and periodical acknowledgement, excessive overhead and delay may occur.

In this thesis, we propose an overlay token ring protocol (OTRP). The protocol works by grouping vehicles running on the road into multiple overlapped virtual rings with a token in each of them as the right for transmission and other control functions. Tokens belonged to different rings in the same area contend for the right to transmit but with the sole transmission right in its belonging ring. The components of the ring are dynamically adjusted according to traffic conditions. The OTRP optimizes the IVC performance in both data and safety applications as follows:

1) **Quick access to medium and good fairness in bandwidth:** Ad hoc networks are exposed to low throughput and unfairness problem. In OTRP, since transmissions are conducted in an ordered way and each node is mandatory to release the token for maximum token holding time (*MTH*) that guarantees the quick access to medium. Moreover, the token stays at each node for an equal period of time which contributes to fair bandwidth sharing.
2) **More predictable network performance and reduced contentions:** In OTRP, by passing a token with same *MTH* in each node, the token rotation time is bounded. Furthermore, since there is always only one node is in transmitting, with same traffic dense, the number contending for the medium is the overlapped ring number instead of the actual node number. Bandwidth wasted in collisions is greatly reduced. Each node can get a latest record of ring order from accepted token which contributes to a more predictable performance in vehicular networks.

3) **Robust in vehicular environments:** A series of intelligent algorithms are devised in OTRP to keep rings dynamically adjusted by accepting new nodes, deducting leaving nodes and reformulation when necessary. Even under high mobility situations, nodes can form organized rings to keep communication in an ordered way.
4) **Reliable message broadcast with limited delay:** The warning message has the highest priority once it's generated. Normal node is switched to emergency mode when the token holder receives safety message. The token is then passed as acknowledgement or retransmission request if the arriving node is lack of message. During the acknowledging process, data transmission is not allowed so the acknowledging delay is very short which meets the requirements of safety applications. The emergency message ends when all receive of messages are confirmed.
5) **Inexpensive to implement:** OTRP is an overlay protocol that can work on available MAC protocols. It's more practical than implementing expensive hardware or design a new MAC protocol.

In this thesis, OTRP's performance is evaluated by a probability model. This model is devised based on three key parts of parameters: MAC scheme, ring configuration and vehicle's average velocity. Average access delay, token rotation time and throughput under saturated situations are evaluated on a single ring condition as well as emergency delay. Simulations are conducted to verify the theoretical analysis. The performance analysis demonstrates that OTRP is competent in providing QoS guaranteed performance and supporting emergency dissemination within limit time even when the network topology is changing frequently.

The remaining of the thesis is organized as follows: Chapter 2 provides the vehicular communications network background and detailed literature survey on current proposed VANETs MAC protocols. Chapter 3 describes the main schemes of the proposed protocol in two aspects, the normal mode for data transmission and the emergency mode for safety applications. The analytical model is presented in Chapter 4 and the theoretical analysis is given based on the model. Chapter 5 presents the comprehensive simulation results to evaluate OTRP's performance and to verify theoretical analysis as well. Chapter 6 concludes the research and gives potential research topics on this subject.

Chapter 2 Background and Literature Survey

According to statistical reports, a large number of people die due to traffic accidents. The vehicular communication is designed to give warnings and reminders to vehicles running on the road so as to decrease the fatalities and injuries. Furthermore, it is assumed to provide live road situations and with developing technology, applications over wireless on wheels will also be an emerging area.

There are two ways of communications over vehicular networks, Inter-Vehicle Communication (IVC) and Roadside-to-Vehicle Communication (RVC). IVC is generally defined as communication between two or more on-board vehicles while RVC is the communication between vehicles and the infrastructures such as base stations to gain access to Internet and message relay boxes used to store, process and transmit messages. Generally speaking, those two types of communications are correlated to achieve the complete application. Fig. 2-1 shows the vehicular communications composed of IVC and RVC. Equipped with mobile device, vehicles on the road can form an integrated network by ad-hoc communication mode as Vehicular Ad-hoc Networks (VANETs) to achieve long distance communication as well.

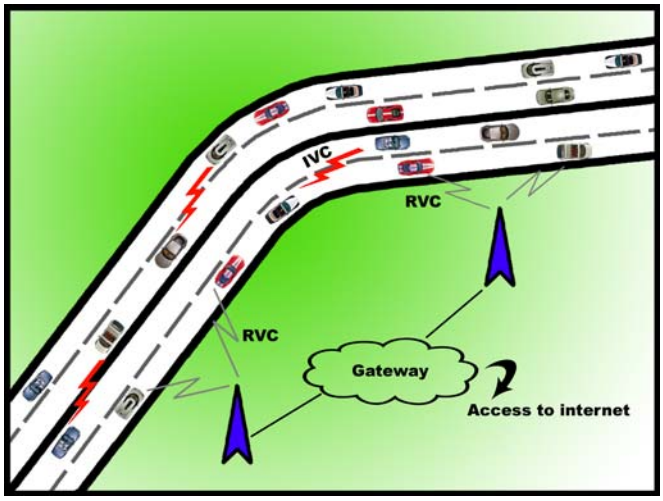

Figure 2-1: IVC and RVC Communications

Since 1980s, Japan Traffic and Driving has begun to research on IVC and till 2000, a series of experiments were conducted and the IVC reference model **Error! Reference source not found.** is proposed for future research. In Europe, a Wireless Local Danger Warning system (WLDW) allows cars to inform each other about the traffic situation, bad weather conditions, road constructions and obscure obstacles, which is included in the context of European integrate project PREVENT. In the

United States, 5.9GHz Dedicated Short Range Communication (DSRC) technology has been reserved for vehicular safety applications. The short range communication covers 200-300m line of sight, however its coverage can reach 1000m by specific directional antenna configurations and high transmission power.

At present, Wireless Access in Vehicular Environment (WAVE) has been widely accepted and is being standardized by IEEE P1609 and IEEE 802.11p to provide low latency wireless communication in short to middle distance. The multi-channel structure in DSRC is adopted by WAVE with one control channel and six service channels. The development of WAVE also makes PREVENT merge WAVE to European standards. Vehicular MESH (VMESH) on the WAVE multi-channel structure is proposed for RVC to improve throughput as a part of PREVENT project.

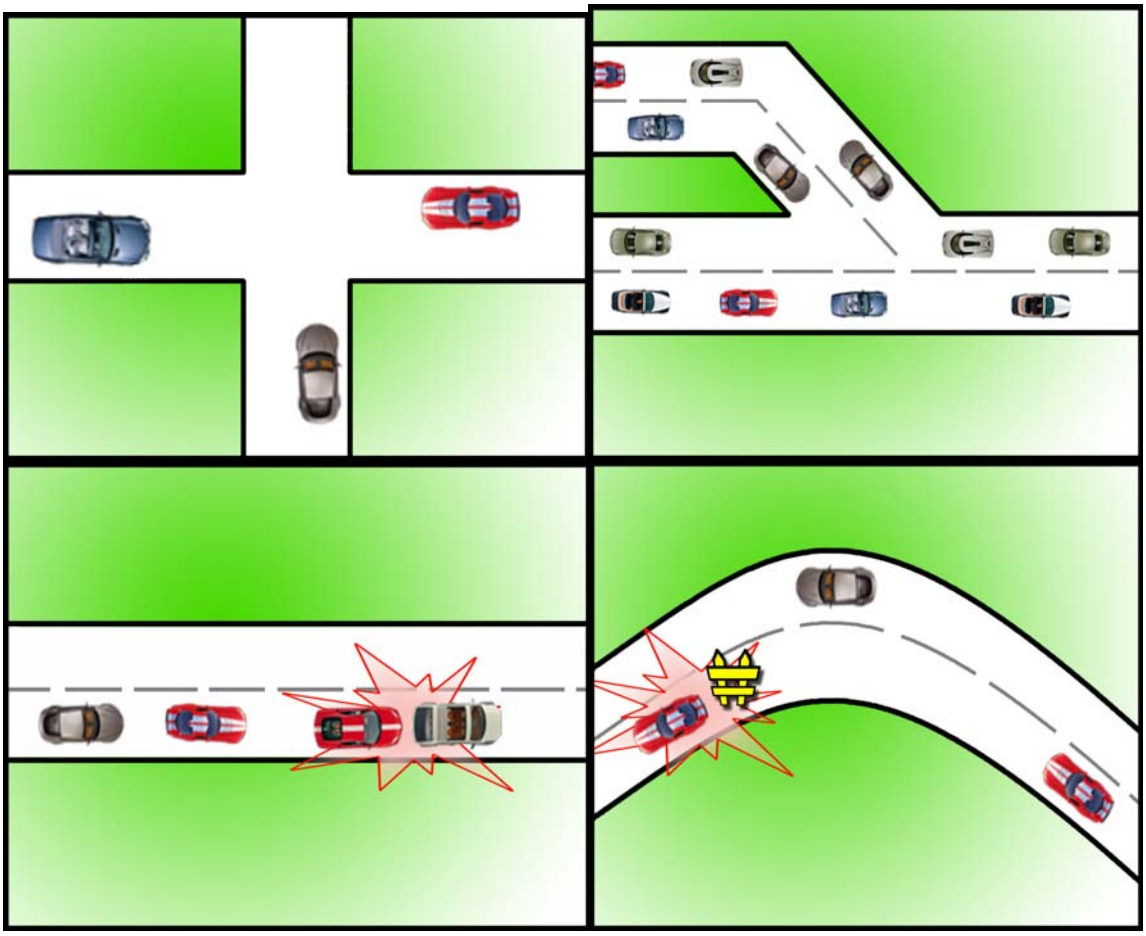

Figure 2-2: Typical Safety Applications on Vehicular Networks

2.1 IVC Applications

IVC applications can be classified into three categories:

1) **Safety application:** Safety applications target to decrease the dangerous potential of driving. For example, if there is a collision happening near the vehicle, warning messages will be disseminated to effective area in short time to make awareness of the event and vehicles can thus decelerate the speed to avoid collisions once they get the message. Rear-end collision warning is one of typical messages in safety application.
2) **Drive control:** Provide instant control information by exchanging with nearby vehicles and data analyzing, such as merging and turning during highway driving control, safe entrance and exist indication, etc.
3) **Data and real-time application:** Provide travel information around vehicle's district such as hotels and gas stations; communicate and exchange information with other vehicles; share resource and internet for entertainment like playing games, etc.

Those applications have specific requirements for vehicular networks:

1) Communication quality: high throughput, low packet loss and low delay.
2) Safety applications: Safety- related applications are delay-sensitive and usually require high reliability.
3) For the drive control application, service priority should be defined according to urgency and orders are queued and executed to achieve coordination function.

Compared to traditional wireless communication mode, power restriction, data storage and time synchronization are no long the main conflicts in IVC thanks to the power system merged in vehicles and GPS location system. Typical safety applications on vehicular networks are shown in Fig. 2-2. They are cross coordination, merging/splitting control, collision warning and obstacle reminder in the turn as from left to right top to down.

2.2 Vehicular MAC Layer Design

Vehicles running on the road accelerate or decelerate at random time, which makes the vehicular network topology quite uncertain. The network instability is considered the biggest challenge for vehicular network protocol design.

IVC based on VANETs needs efficient and reliable protocols to support applications. Several MAC layer protocols have been proposed and demonstrated suitability for vehicular networks.

Popular ones are TDMA-based RR-ALOHA, IEEE 802.11a chosen for DSRC standard by American Society for Testing and Materials (ASTM), IEEE 802.11p (WAVE) specially designed for vehicular communications and has amendments on MAC/PHY layer specifications for safety applications and the directional antenna based MAC protocols devised to decrease collisions by dividing space into multiple channels. At present, the MAC protocol for vehicular networks hasn't been specified and researchers are seeking a promising MAC protocol which should also be easy-implemented and low-cost. In the following, we demonstrate the candidate MAC protocols for VANETs.

2.2.1 IEEE 802.11a/b/g

IEEE 802.11x is the series of standards defined for current Wireless Local Area Network (WLAN). It's based on CSMA/CA mechanism with slotted exponential back off scheme. IEEE 802.11x is a family and 802.11b/g/a are the most popular among current WLAN deployment. 802.11b/g both work on the 2.4GHz unlicensed frequency band. 802.11b's raw data rate can reach 11Mbps and 802.11g's can reach up to 54Mbps. 802.11a is assigned 5GHz unlicensed frequency band and with OFDM modulation, it can reach maximum raw data rate to 54Mbps. The different frequency band makes 802.11a less interference and high raw data rate but the penetration ability compared to 802.11b/g is weakened, which means that the effective range of 802.11a is smaller.

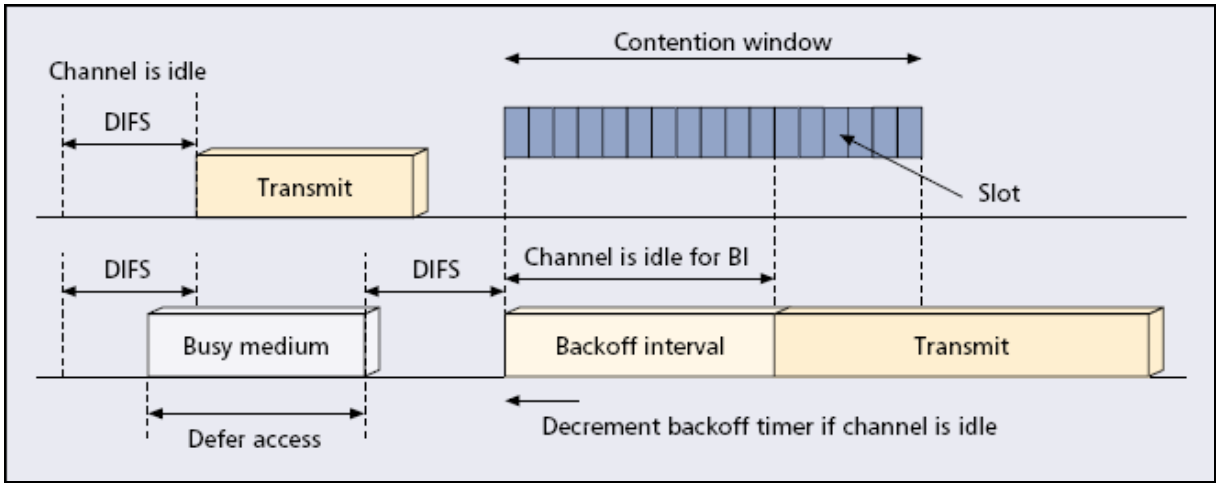

Figure 2-3: IEEE 802.11 Distributed Coordination Function

There are two mechanisms in IEEE 802.11x, Distributed Coordination Function (DCF) and Point Coordination Function (PCF). At present only DCF is widely used in WLAN. DCF mechanism is shown in Fig. 2-3. It has two mechanisms, basic mechanism and RTS/CTS mechanism. In basic

mechanism, when a node is going to send a packet, it first senses the status of the channel. If it's idle for continuous DIFS time, the node goes into the back off stage. Back off counter is a number uniformly chosen between 0 and Contention Window (CW), which is first set to a minimum number specified in the standards. Back off counter is decreased by one if the channel is sensed idle for a SLOT of time, if channel is busy, the counter is frozen till it is idle again. The node sends the frame when the counter becomes zero. For each successfully transmission, CW will be reset to minimum value. On the other hand, for each failed transmission, CW will be doubled till it reaches to maximum value.

When the destination node receives the frame, it will send back an acknowledgement frame (ACK) to the sender after SIFS duration of time. Since the ACK is correctly received, the transmission round trip is finished.

RTS/CTS mechanism is similar to basic mechanism, but instead of sending a packet after back off counter is decreased to zero, it sends a RTS frame to the destination node. A CTS frame is sent back to confirm the set up of connection from the receiver SIFS after receiving RTS. RTS/CTS frames contain the information of the duration this transmission will occupy the channel, by hearing RTS/CTS frame other nodes contending for the same channel update NAV as their latest time for next trial and when receiving an ACK, NAV is set to zero. NAV is a virtual vector to indicate the time duration channel is busy. RTS/CTS involves more overhead, but it solves the hidden terminal problem, and collisions happen only between RTS/CTS frames rather than between frames.

IEEE 802.11a/b/g can work in two modes, one is that nodes are connected to infrastructure such as access points or base stations; the other is that nodes communicate with each other directly or via other nodes without involvements of infrastructure, i.e., ad hoc mode. The 802.11x working in ad hoc mode are deemed for vehicular networks. Because of the deep research, simple deployment and wide spread of WLAN, IEEE 802.11x is still a competitive MAC protocols for IVC.

2.2.2 IEEE 802.11p

The IEEE group is working on the specifications for safety applications on the DCSR frequency band, which is named IEEE 802.11p or WAVE (Wireless Access in Vehicular Environments) as amendments on MAC/PHY layer. IEEE 802.11p standardizes safety specifications on both IVC and RVC within the range extending 1000m and takes the high mobility environments into considerations. On PHY layer, it works on 5.850~5.925GHz licensed frequency band and uses

OFDM modulation system. IEEE 802.11p MAC layer is based on the same core mechanism CSMA/CA as other IEEE 802.11x protocols and can reach raw data rate to 54Mbps.

IEEE 802.11p takes the similar channel allocation scheme as DSRC with one control channel (CCH) reserved for control information and six service channels (SCH) for data transmissions. The CCH is designed for control frames and safety application frames while SCH is for normal data service. By multi-channel operation, the safety warning message will not be delayed while data application can run at the same time. Enhanced Distributed Channel Access (EDCA) specified in IEEE 802.11e is applied to differentiate priorities of service channels. EDCA achieves QoS support by mapping different traffics to different virtual stations, with each station assigned a parameter to signify its priority. IEEE 802.11p is planed to be published and finalized in April 2009.

Table 2-1: Main Parameters for IEEE 802.11a/b/g/p

	802.11a	**802.11b**	**802.11g**	**802.11p**
Maximum Data Rate	54Mbps	11Mbps	54Mbps	54Mbps
RF Band	5GHz	2.4GHz	2.4GHz	5.9GHz
Channel Width	20MHz	20MHz	20MHz	75MHz
Number of Channels	23	3	3	7
Modulation Technology	OFDM	DSSS,CCK	DSSS,CCK, OFDM	OFDM
Different Data Rate Configuration	8	4	12	8
Typical Range	75feet	100feet	150feet	300feet

WAVE also takes the safety application requirements into standardization on the traffic situation statistics. Further more, in Europe, the PREVENT project research group WILLWARN are keeping pace on MAC/PHY protocols development with North America and begins to standardize WAVE to European market. Table 2-1 shows the main MAC/PHY layer parameters of IEEE 802.11a/b/g/p.

2.2.3 Vehicular Mesh Network MAC

The WAVE ability in supporting high throughput has been questioned in [43] and a novel MAC protocol Vehicular Mesh Network (VMESH) MAC is proposed based on the multi-channel structure of WAVE, which applies a reserved TDMA scheme in SCH to be throughput-efficient. The throughput supportive communication is between Roadside Unit and vehicles passed by.

The following mechanisms are proposed in VMESH:

1) VMESH further divides CCH into a beacon period (BP) and a safety period (SP). The BP is divided into slots and each vehicle passed by chooses a unique slot. The BP slot is used to broadcast beacon message that includes vehicle's information. By beaconing scheme, each vehicle is able to keep awareness of neighboring nodes and further coordinates resource allocation in SCH. SP is reserved for safety application only. In this way, interference between control messages and management messages are reduced.
2) A reservation TDMA scheme is applied in SCH. Exchanging reservation information by beacons between the node and Roadside Unit (RSU), bandwidth is coordinated in a ordered way thus improve the throughput.

In implementing these mechanisms, VMESH achieves reserved resource allocation in RSU and wise coordination between vehicles while adhere to the multi-channel structure of the MAC protocol WAVE.

2.2.4 Reserved Reliable-ALOHA

Reserved Reliable-ALOHA (RR-ALOHA) is proposed to solve some significant problems in ADHOC networks. It is a completely distributed mechanism without any central control and provides reliable MAC broadcast within one-hop on a slotted mechanism. RR-ALOHA also solves the problems of hidden and exposed terminals in VANETs in a TDMA-based way.

Specifically, RR-ALOHA protocol is proposed in [1] and [28] that inherits some characters of Reliable-ALOHA. RR-ALOHA can work either on the ULTRA-TDD physical layer such as UMTS TDD or asynchronous physical layer as IEEE 802.11. RR-ALOHA is a slotted-channel allocation mechanism which each node has a reserved channel named Basic Channel (BCH) for transmitting the channel utility information Frame Information (FI). BCH can be heard by all nodes within one hop and it's also used for other signaling and payload information. FI provides the latest period of channel occupation situation in the frame, i.e., if a slot is occupied, it will be tagged as BUSY with the node identity and otherwise it will be tagged as FREE. Once a node occupies one of the slots, the same slot of next round is reserved for it as well. Each node must get a BCH to be active. By BCH and FI, nodes can understand the channel allocations and pick up a FREE slot for transmission. The transmission by a station is correct if all the received FI tagged the same slot as busy by its identity. Fig. 2-4 shows how FI signifies the channel information to different nodes.

It can be sees that each node can only know the slot occupation information in its radio range, and nodes within overlapped area can get the information of both clusters. For example, in FI-3, node 5,

2, 4, 6, 3 are tallied as busy nodes in specific slots, and those slots are reserved in the next frame for them respectively. The transmission should be heard by all the nodes in coverage and if a lack of notice appears in the one of those FI, it means that the transmission fails.

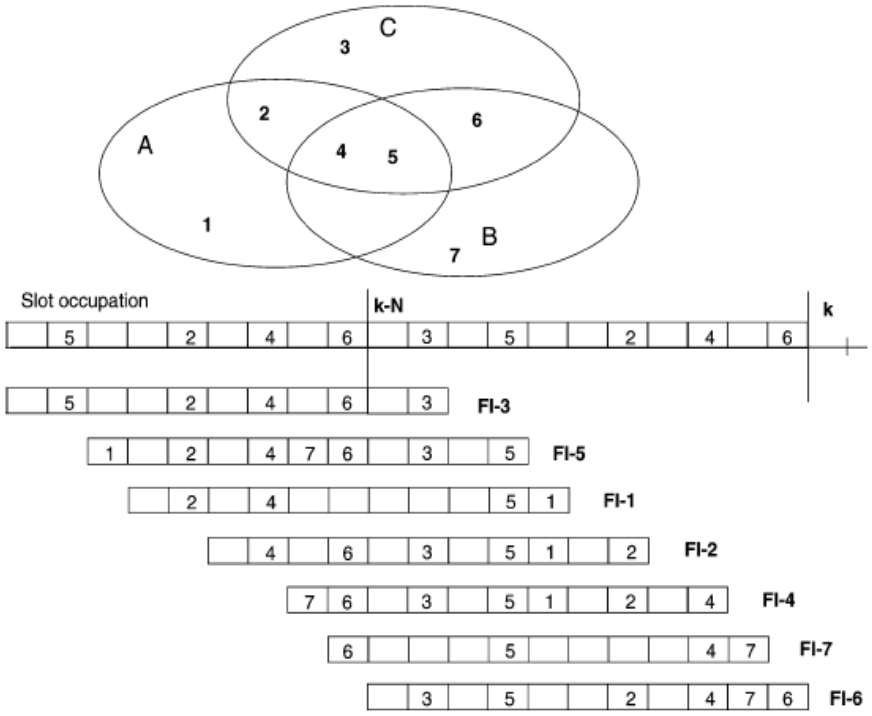

Figure 2-4: Single Hop RR-ALOHA Communication

RR-ALOHA can be extended to multi-hop communications and this is achieved by the nodes in overlapping area to arrange and transmit FI to both one-hop clusters. The FI can show the slots allocation in the multi-hop area but different from the one-hop scenario, same slot can be tagged with multiple node identities since those identities do not interference with each other. In addition, if the bandwidth of the channel is insufficient for a specific application, free slots can be added to support the service. This bandwidth reservation policy supports some applications that require high bandwidth in ADHOC networks.

The dynamic TDMA scheme is recommended by the European standards and is proven to be efficient for inter-vehicular networks since it does not have power constraint for synchronization equipment as GPS. However, RR-ALOHA has not been standardized and put into implementation

thus a large number of experiments are needed. Furthermore because of the slotted structure, implementation of accurate synchronization is also a problem.

2.2.5 Token Ring Protocols

Token ring protocols work as peer-to-peer protocols on any MAC or network layer. The token ring concept was first applied in wired network token bus protocol IEEE 802.4, which assumes only the node holding the token has the right to transmit. But recently, the token ring protocols are investigated their effectiveness in IVC due to the high requirement on an efficient approach in organizing nodes in vehicular environment In the following, Wireless Token Ring Protocol (WTRP) and Reliable Neighborcasting Protocol (RNP) are demonstrated.

2.2.5.1 Wireless Token Ring Protocol (WTRP)

Wireless token ring protocol is proposed for wireless mobile ad hoc networks by organizing nodes as a logical ring. It dynamically includes the processes of joining and leaving processes and guarantees Maximum Token Rotation Time (MTRT) and bandwidth by bounding the time token stays at each node. The latest version of WTRP [7] was published in 2004, which describes the complete mechanism, implementation and performance analysis compared to IEEE 802.11 protocol.

WTRP supports partial connection by specifying the token frame format with fields signifying token type and functions. A node can be belonged to one or more rings and assigned multiple sets of properties. Several control mechanisms are also devised at each node, such as building a connectivity table for looking up its previous and next node; joining control and leaving control for adding and deducting process of the ring.

Different priorities are assigned to tokens by sequence number field in the token frame so that when multiple tokens are discovered, the lower priority one will be dropped. The ring recovers by excluding the leaving nodes from the ring and set the nearest accessible node as successor by looking up the connectivity table. When a node is in FLOAT status that is not belonged to any ring, it senses for the strongest ring signal and waits for the SOLICIT_SUCCESSOR token to join the ring if the NoN (Number of Nodes) doesn’t reach to maximum value.

The WTRP applies implicit acknowledgement, i.e., when a node sends frames, it means that the token has been successfully transmitted to it, and by hearing the transmissions, connectivity table is built correspondingly of the order of transmissions. The node in the ring gets aware of the node

number in the ring by the following way. There is a sequence number field at each token format. The sequence number is set to zero once it arrives at the owner node of the token, and is increased by one when it passes by a node. When the token comes back to the owner, NoN is calculated by sequence number difference accordingly. Fig.2-5 shows how nodes utilize connectivity table to calculate the NoN.

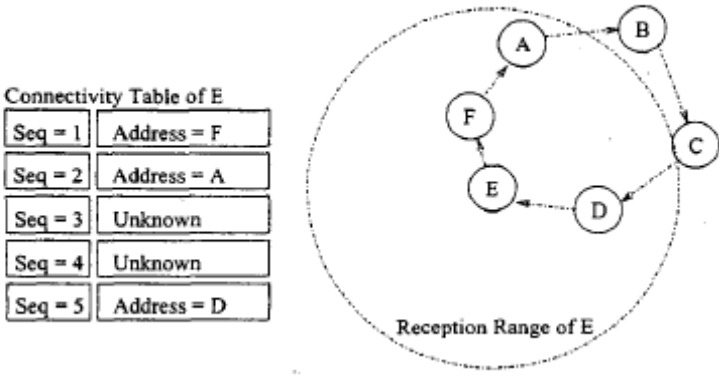

Figure 2-5: Using Connectivity Table in WTRP to get the Node Number

WTRP has joining and leaving processes to adapt to network topology change, which are shown in Fig. 2-6 and Fig. 2-7.

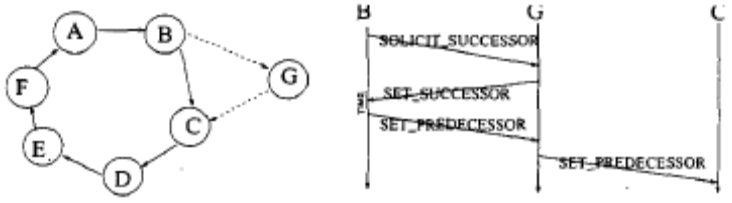

Figure 2-6: Joining Mechanism in WTRP

Figure 2-7: Leaving Mechanism in WTRP

The most noticeable character WTRP advocates is the guaranteed bandwidth, bounded token rotation time and fairness through ad hoc networks. By performance analysis, the WTRP has better performance in saturated throughput under high traffic conditions by decreasing the collisions and more fair in an ad hoc network. Network performance is more predictable than IEEE 802.11x by different timer for different actions. Furthermore, WTRP takes the network changing into consideration and keeps dynamic control in joining and leaving process for nodes. However, the protocol has some drawbacks. First the organization scheme does not fit quickly changing vehicular environments that tends to frequent ring reformulations. Its application for IVC is not investigated. Furthermore, WTRP does not provide a reliable and high-efficient scheme for safety applications. In summary, WTRP is innovative in wireless application of token ring protocol but can not satisfy the IVC demands.

2.2.5.2 Reliable Neighborcasting Protocol (RNP)

RNP is belonged to the series of reliable multi-cast and neighborcast protocols proposed by [4]. Reliable Broadcast Protocol (RBP) is first designed and implemented. Time-driven Reliable Multicast Protocol (T-RMP) constrains delay bound by sending token periodically instead of event-driven. Mobile-RBP (M-RBP) takes the high dynamic network topology into consideration by a voting process to add or remove nodes from the group. RNP, however, is an overlay on M-RBP, but put neighbouring nodes by location into a cluster for broadcast. By the overlapped area of clusters, the message relay to the whole network is accomplished. It's specifically designed for IVC and is an overlay that can work on any layer providing reliable neighborcast function. In the following, we give details of this set of reliable broadcast protocols.

RBP: RBP guarantees that all the receivers have all the messages by sequentially passing the token to each receiver. A receiver only accepts the token when all the preceding acknowledgements and corresponding messages are successfully received.

Sources continuously transmit message Ms at a regular interval until it receives an acknowledgement or decides that the token site is not open, which needs reformation. Receivers take turns acknowledging messages by passing a token. A control message t from assumed token site r takes three functions as Fig. 2-8 shows:

Acknowledge to the message Ms and assigns it sequence number t.

Acknowledge to site r-1 mod m that token has been successfully transmitted.

Pass the token to site r+1 mod m.

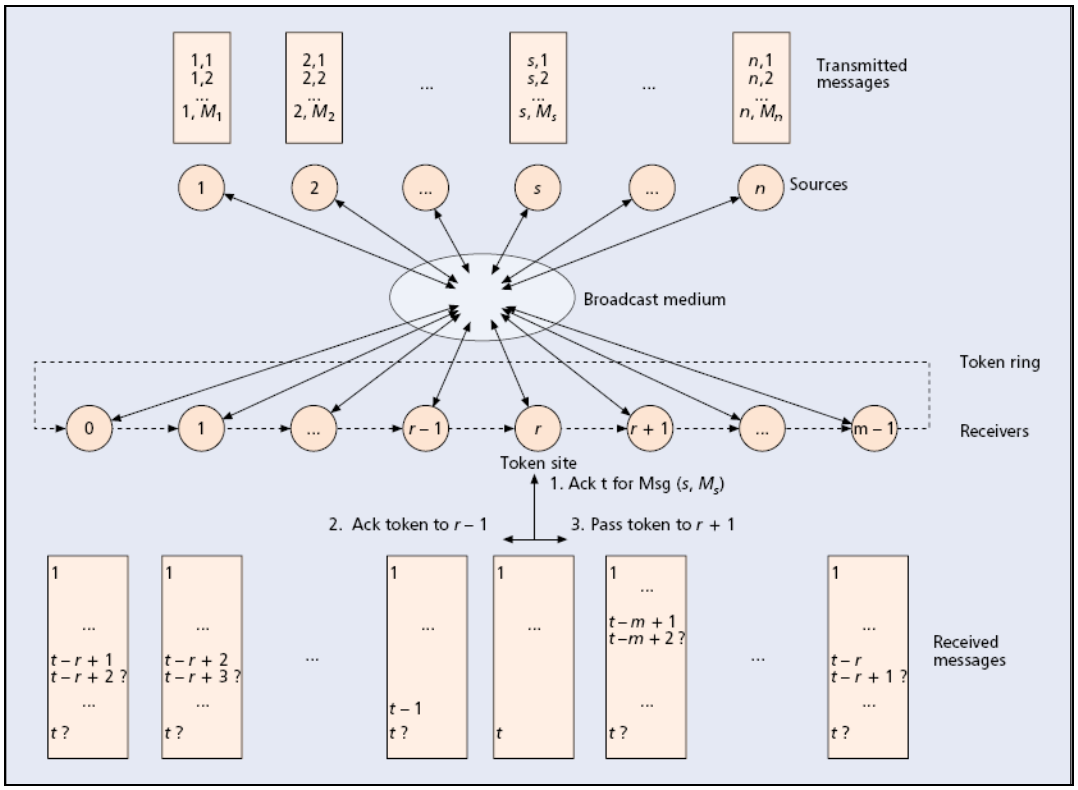

Figure 2-8: Reliable Broadcast Protocol

Token site r applies a positive acknowledge. It continuously sends t until it get acknowledge t+1 or greater or it receives a separate token acknowledgement. The token stays at the receiver until a new message enters the system, which is event-driven. The node receives the token is also responsible for retransmission. No more control messages are sent until a missing message is detected. Then the receiver periodically sends request for the message till gets it. With the passing of token, the token site can infer other receivers' information.

T-RMP: It is time-driven instead of event-driven to compensate defects of RBP that can't guarantee delay. It uses similar token pass and retransmission mechanism as RBP. The e^{th} token is transmitted at time $t_e = t_0 + e\Delta T$. When there are multiple messages that have not been acknowledged, the acknowledgement contains a list of unacknowledged messages since last pass of token. Furthermore, T-RMP initiates the acknowledge recovery process shortly after the acknowledgement is transmitted, instead of waiting for next acknowledge. Assume T_R to be the round trip delay and $N_{\max}$ is the maximum retransmission request time, a receiver starts the recovery process at $T_R/2$. T-RMP sets $\Delta T \geq (2N_{\max} + 1/2)T_R$ to ensure that next token can recover all missing acknowledgements and the messages that were acknowledged.

T-RMP guarantees that all receivers acquire and sequence the message within ΔT after the message is acknowledged. Assume that the source retransmits message $N_{\max}$ times before entering into reformation process by an interval ΔT , we can get the delay bound that a message is broadcasted and placed in right order to all the operable receivers as $(2N_{\max} + 1/2)T_R(N_{\max} + 1)$ seconds, thus achieve the reliable transmission within limited time.

M-RBP: M-RBP is based on the T-RMP and takes the frequent changing network topology into consideration. The receivers use a distributed voting procedure to determine if some nodes miss acknowledgements messages or if the receivers already leave the group.

M-RBP decides the following by voting: which receivers have left the group, which acknowledgement number is in the set of valid acknowledgements and which source messages are successfully sequenced. For instance, if the e^{th} acknowledgement is scheduled to be transmitted at t_e , the acknowledgement transferred at $t_e + T_A$ includes a vote on whether or not the acknowledgement at t_e is really transmitted, where $T_A = (2N_{\max} + 1/2)T_R$. Given there are m receivers in the group, at $t_e + 2T_A + m\Delta T$, all the acknowledgements should have been voted and recovered. The result is then tallied at each receiver.

A similar vote is started at time $t_e + (2N_{\max} + 1/2)T_R$ for the message acknowledged by e^{th} acknowledgement to decide which messages are in the final sequence. From the results of the vote, the receiver can either have the acknowledgement or does not have or it does not vote because the receiver left the group.

A receiver joins a group by sending broadcast request and waits for acknowledgements and votes. If more than half of the receivers leave the group during a token passing round, the group starts to reform by accepting nearby receivers instead.

RNP: RNP is a distributed mechanism on ad hoc networks without infrastructure. It is designed for IVC to guarantee the neighborcast reliability; delay bound, ordered messages sequencing and the time when all the other nodes get the message. RNP considers the vehicular network by overlapping groups with each vehicle and its neighbouring group. A vehicle's neighbouring area is defined as certain range around it as shown in Fig. 2-9.

RNP is an overlay on overlapped M-RBP groups and provides a scheme how this paradigm works. The inadequacies of RNP are obvious. First, although it can provide reliability and same ordered messages by time-driven and aggressive acknowledgements, constant retransmission of ACK messages and multiple acknowledgements for the same message cause tremendous overheads. Secondly, RNP doesn't explain the scheme that can avoid collisions by this aggressive broadcast mechanism either. Finally, there is no specific performance analysis shows RNP's superiority over other MAC protocols. In general, deep and comprehensive research needs to be done on RNP.

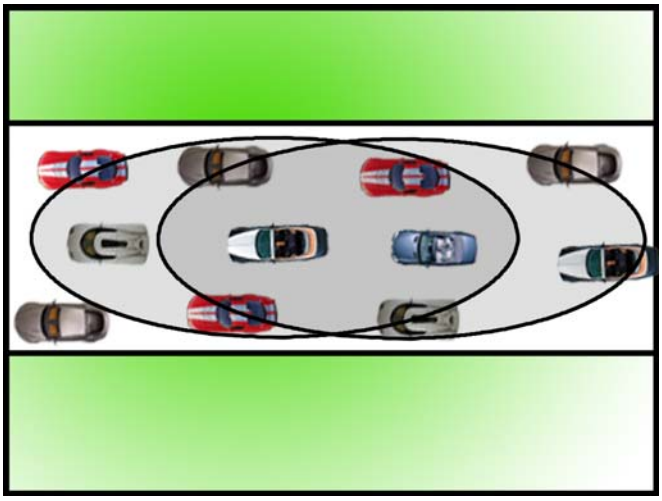

Figure 2-9: RNP Neighbourcast Group

2.3 Research Motivations and Objectives

Although several IVC MAC layer protocols have been proposed based on the experience of previous ad-hoc network protocol design and the predefined safety application requirements, the quickly

changing topology is still the biggest challenge for guaranteed QoS and reliable safety message dissemination. Furthermore, the proposed MAC protocols are usually suitable to a specific scenario rather than various conditions on the vehicular networks. In this section, the main requirements of IVC MAC layer protocol are addressed and the motivations and objectives of the research are demonstrated.

2.3.1 IVC MAC Layer Challenges

The main challenges to IVC MAC protocols are how to organize vehicles on road in a communication-efficient way and provide QoS for both applications that is robust to quickly changing network topology.

Insufficiency of current MAC protocols:

1) The IEEE 802.11 protocols are considered mature in research and implementation, hidden terminal problem has been released in ad hoc networks, but for IVC applications, some restrictions still exist. First, in ad hoc mode, there is no central control and network performance is unpredictable which highly depends on facts including both network topology and node performance. Thus under this free contention scheme, it can not guarantee the time limit for reliable emergency message broadcast and bandwidth for real-time and other data applications. Secondly, the unfairness problem is inherited from multi-hop wireless networks that nodes can not share the bandwidth in a fair way. Unfairness distribution decreases the network performance and utilizes the bandwidth in an inefficient way.

2) Regarding RR-ALOHA, issues related to mobility and accurate implementation of synchronization need deep research. Moreover the inherited disadvantage of TDMA is the inflexibility in allocating slots. In RR-ALOHA, the number of slots in each frame should always be larger than the number of vehicles in the same radio range or some nodes can’t access the channel for service. In addition, when the network is not very busy, bandwidth is not fully utilized and the efficiency is eliminated.

3) Directional antenna based MAC protocol uses space reuse to increase throughput by decreasing collisions. However complicated deployment and high cost impede it to real situation

4) WTRP is designed to provide QoS guaranteed data service in wireless networks . However, the proposed protocol is quasi-stationary which may not suit the high speed changing vehicles. To be more specific, first, in WTRP only the token owner can know the node number in the ring after a rotation time, which is challenged by the quickly changing network topology. Second, there is not a ring recovery scheme devised in WTRP if the node with the token leaves the ring. Thirdly, only on node can be added each time which is inefficient in vehicular environments. Managing the ring topology by the distributed way described in [7] can not adapt to the complicated topology change in vehicular networks. Finally, WTRP does not provide a quick and reliable broadcast scheme which is required by IVC safety-related applications.

In summary, a promising MAC protocol is necessary to cover the demands of IVC which is easy and inexpensive to implement. A qualitative comparison of current proposed VANETs MAC protocols is presented in Table 2-2.

Table 2-2: Qualitative Comparison of Proposed MAC Protocols

	IEEE 802.11x	WTRP	RNP	RR-ALOHA	VMESH
Contention scheme	CSMA/CA	Token-based	Upon broadcast MAC	TDMA	CSMA/CA
Implementation maturity	Mature	Linux implementation	Not implemented	Medium	Not implemented
QoS	No	Bounded delay	Reliable broadcast	Medium	High throughput
Synchronization needs	No	Yes	Yes	Yes	Yes
Mobility	Medium to high	Quasi-stationary	Medium to high	Medium	Medium
Reliable broadcast	No	No	Yes	Yes	No

2.3.2 Problem Formulation and Research Objectives

According to our survey on IVC MAC protocols, the MAC layer for IVC should have following features to support safety, data and real-time applications with guaranteed QoS under vehicular environments.

1) The MAC protocol can support time-bounded message transmission for drive control by different priorities. It can also disseminate warning message in time limit with great reliability. Therefore, the MAC delay for the safety application service should be minimized and the percentage of nodes receiving the message over the total vehicles within effective range should be maximized.
2) Short delay in accessing the medium, i.e., the MAC delay between a frame is at the head of the buffer to the time it's successfully sent should be minimized.
3) High throughput and fairness are also important criterion for data service.
4) Adaptive to the quickly changing network topology in a robust way. This is usually based on the efficient communication group in which vehicles are flexible to exchange between different groups by their movements.
5) Simple and inexpensive to implement. Since the cost affects the acceptance of the technology and the protocol should not be totally new which will delay the deployment.

In order to achieve the above goals, IVC has following key problems pending to be solved:

1) Organize the cluster in an efficient way that is flexible to the VANETs dynamic topology. Current proposals suggest a node leader named cluster header to perform the management function, but there is not a recognized approach on how to assign the header. In our protocol, however, the cluster header is passed in turn instead of a fix node to survive the quickly changing topology.
2) Release the contention and provide QoS to data service. Since when the traffic is dense, severe contentions significantly decrease the performance, a scheduling scheme is required to make the transmission in a more ordered way to reduce collisions and make the network performance more predictable.
3) Provide quick and high reliable broadcast scheme for safety-related messages.
4) Adaptability to the speed. The nature of vehicular network needs quick adjustment to access medium which should be covered in the protocol.

Therefore, we design an overlay MAC protocol named Overlay Token Ring Protocol (OTRP) which meets the requirements of IVC as describing above. The protocol is designed for IVC with

vehicles driving along the same direction such as the case in highway. Normal and emergency modes are devised in OTRP to meet requirements of data applications as well as safety related applications.

Chapter 3 Protocol Description

OTRP can work on any MAC layer with broadcast function and it works by organizing the vehicles into overlapped communication groups. Medium access of each node is determined both by token assignment and contention. To be specific, within a group the node holding the token has the sole transmission right while under overlapped rings situation, tokens still need to contend to access medium. In the emergency situation, the token performs as the acknowledgement to the safety related message at each node and request for retransmission when missing a message occurs.

In this chapter, the system model for OTRP is described. Problems the protocol is targeted to resolve are formulated. Details on the initialization and operation of the protocol are demonstrated. And dynamic recovery scheme for keeping ring structure robust in varying topology is presented.

3.1 System Model

3.1.1 Network Topology

We consider a 2-dimensional homogeneous network model. For IVC, the whole network is divided into overlapped clusters by communication range.Clustering concept is widely used in network topology in IVC. The reason to propose the clustering concept is due to the fast changing topology of vehicular networks, the application and service are usually based on the communication with nearby vehicles. Generally, clusters can be divided into:

1) Dynamic cluster, where nodes are moving while keep relatively stationary positions. In a dynamic cluster, a node can stay with nearby nodes for a certain period of time.
2) Quasi-stationary cluster aims at cooperation among fluctuating network participants, which roadside infrastructure covers a certain area.

In IVC, we only consider dynamic clusters that vehicles in nearby range are virtually grouped. RVC is supported by roadside infrastructures which can be a gateway to access Internet.

In the proposed OTRP, vehicles in a cluster are organized as one ring or several overlapped rings as shown in Fig. 3-1, and each vehicle is belonged to one or more rings. The ring has an upper limit for the number of nodes in it. In addition, nearby *FREE* nodes are ready to join the unsaturated ring. If there is only one ring, the node holding the token has the right to transmit. If several nodes with tokens are in the same radio range, they contend for right of transmission. Since vehicles are moving at high speed, leaving and joining the ring process happen all the time, but the ring structure sustains

by the designed schemes to make nodes keep connection and share the bandwidth. There is an order list in the token which is updated at each token holder. By passing the token, nodes keep awareness of the latest ring topology from the order list.

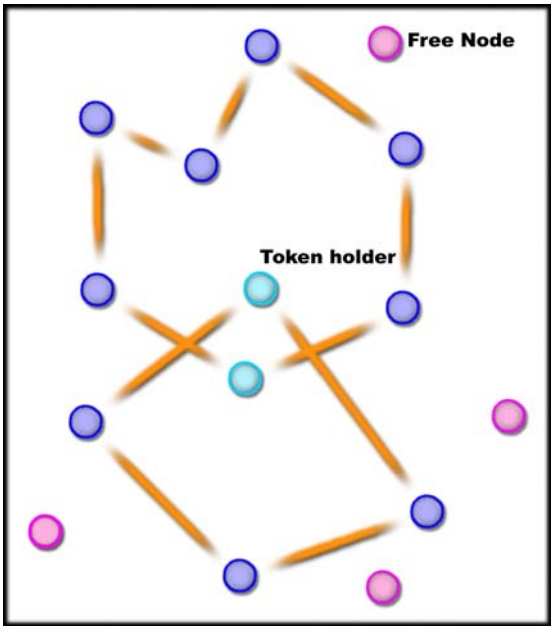

Figure 3-1: Overlapped Logical Ring Structure in a Cluster

3.1.2 MAC and Channel Description

OTRP can be implemented on any MAC contention scheme which has broadcast function. Fig.3-2 shows the layer OTRP works. The MAC scheme is mainly used to avoid collisions when multiple tokens exist in the same radio area. For instance, by IEEE 802.11 protocol, two coexisting tokens obey the MAC contention scheme CSMA/CA to contend for transmission. Thus only the node holding the token and winning the contention can transmit. The OTRP provides some additional timing and control on MAC layer, for example, nodes have a timer to be aware of the next token arrival time to deal with ring recovery issues.

3.2 Assumptions and General Description

OTRP is developed under the following assumptions:

1) OTRP is devised to be implemented to the environments where the comparative moving speed of vehicles is not very large.

2) The node with the token has the sole right for transmission in the ring. Thus within a ring only a node is transmitting, except the situation when the normal mode is switching to the emergency mode, where the emergency node has the highest priority.
3) There are three main statuses for the nodes: *FREE*, *INRING_IDLE* and *INRING_BUSY*, which correspond to the status that the node is not belonged to any ring, the node is belonged to a ring but not holding the token and the node is holding the token at the moment. For the status *FREE* nodes, before they join a ring, they can only transmit responding message to OPEN tokens so as to join a ring.
4) Nodes can hear the transmission activities within its radio range.
5) The nodes within same radio range can reach each other, there is no channel interference, i.e. nodes keep constant transmission rate without taking into account the signal fading.

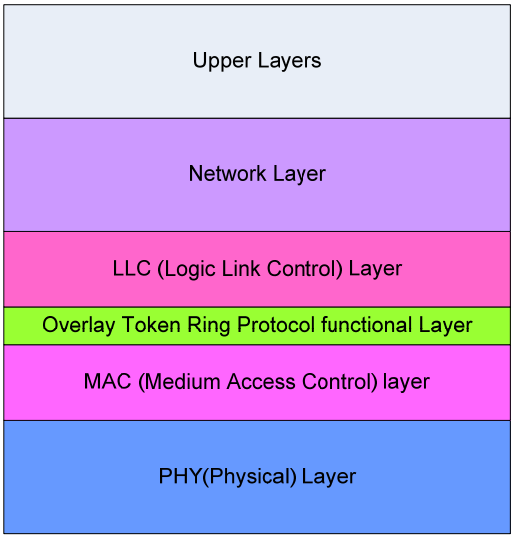

Figure 3-2: OTRP Network Architecture

Upon above assumptions, we define two modes in OTRP: one is the normal mode and the other is the emergency mode. For the normal mode, the token is passed in the ring as the right for data transmission. The upper bound of each data transmission is Maximum Token Holding time (*MTH*). For the emergency mode, where an emergency message is disseminated to warn surrounding vehicles of the dangerous situation, the token performs as the acknowledgement of the emergency message. It is also used as a request for retransmission if missing of the message is found. The ring is dynamically adding and deducting members to fit the dynamic network topology. Order List (OL) in the token field is updated accordingly to keep the latest ring information.

3.2.1 Operation of OTRP

Fig. 3-3 shows the overall OTRP operations under dynamic vehicular environments. There is a communication area rounded by the square. Two rings exist in the it with 6 and 4 nodes respectively. The current token holder of the unsaturated ring is sending out OPEN token to accept surrounding *FREE* nodes. A node in the lower ring is leaving the communication range at the same time. Details are described in following sections.

Ring Initialization: The initialization is the process a ring is formulated. It happens when *FREE* nodes fail to join a ring for T_R. This can be caused when the node is unable to detect a ring nearby or fails to win the contention to join a ring or the ring detected is saturated in T_R. Under the circumstances, the node will generate a token and perform as a "seed" and set status *INRING_BUSY*, then by accepting surrounding *FREE* status nodes, the ring is enlarged. We set the time T_R a little longer than the duration the token is passed a cycle to prevent the situation that too many unsaturated rings exist without *FREE* nodes to join. In this case, more nodes are contending for the medium and the efficiency of medium utilization is decreased.

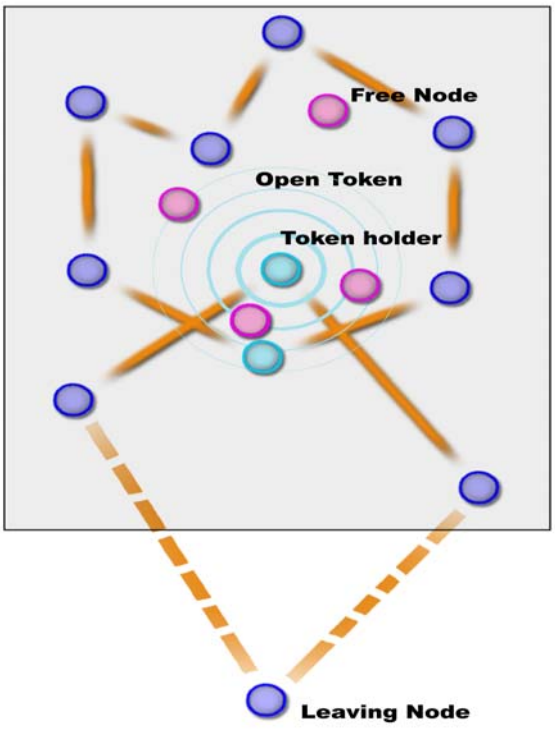

Figure 3-3: Overall OTRP Operations in IVC

Control Messages: The tokens perform as control messages in OTRP. The control messages are classified based on their functions. Five types of control messages are defined and the type is represented in the frame control field (FC) in the token frame. The type of control message is modified when necessary. Defined control messages are as follows:

1) Token as the right to transmit data: When the token resides at a node, it means that *MTH* time is allocated to the node for data transmission.
2) OPEN token: The OPEN token is sent after data transmission and under the condition that the node number in the ring dose not reach maximum. Nodes in *FREE* status can only respond to OPEN token by contention.
3) Responding Message (RM): The responding message is sent when *FREE* nodes detect the OPEN token; it contains the information of the node address.
4) Acknowledgement Token (ACK): Control message is modified to acknowledgement token when the token holder hears an emergency message. There is a field in the control frame indicating whether the node gets the emergency message.
5) Request for message token (RQ): It is used when an acknowledgement token confirms that a node does not get the emergency message. The ACK is modified to RQ and is sent to its nearest node as a request for retransmission of emergency message.

In summary, the token format contains following information: message type, ring ID, sequence number, source address, destination address, the acknowledgement field and reserved field for the OPEN token and latest OL so it can access next node by reading the token.

Token Frame Format:

FC	SN	SA	DA	RING_ID	OL	ACK	RF
1	4	6	6	1	60	1	6 bytes

FC: Frame Control: Define the type of token or emergency warning message type.

SN: Sequence Number: Distinguish different tokens.

SA: Source Address: The address of the source node.

DA: Destination Address: The address of the destination.

OL: Order List: The latest version of ring order list.

RF: Reserved field for *FREE* nodes' addresses.

ACK: Indicate whether the node receives the emergency message.

RING_ID: Distinguish tokens from different rings.

Management of Order List: Each ring member keeps a history record of the transmission activities it can hear named address list. The address list includes all the token transmission nodes' addresses by the time order and its belonging ring ID. This record is built for the node to keep awareness of the ring topology such as the node number and the transmission order. The address list is updated dynamically on surrounding token transmissions and is maintained by following rules:

1) The list contains the address of token transmission nodes and corresponding time for a valid period of time, so the latest ring construction can be tracked and the out-of-date information will not be kept.

2) The host node can get the ring information such as node number and ring order list by looking up the history. To be specific, the ring order list is defined by the cycle with latest unrepeated node addresses, which is the order for a whole rotation. The node number is obtained by the number of nodes in this cycle.

3) When joining process happens, the list is updated by adding newly joining nodes between host node and the next node to be involved in the ring.

4) If a newly joining node finds its address in the address list, the previous history column is deleted in order to avoid "breaking ring" results, which the big ring is broken only involve part of members in. In this case, other members still keep *INRING* status but have no chance to get the token.

A specific example is given below:

We assume five nodes A, B, C, D and E are originally in the ring with ring size 6, and token is passed from A. The original ring order list is A->B->C->D->E. During the token passing process, assume C leaves the radio area and F, G join between A and B, C and D, respectively. So the address lists for all the involving nodes are given in Table 3-1. At each node the OL is updated before passing to the next node as well.

From the address list of each node, the node can configure the latest ring topology by unrepeated appearance of node address sequence. The OL field in the token is updated instantly to keep most recent ring information for nodes to refer. Once a token arrives at a joining node, it can transfer the information of current ring topology to the joining node. And if a node is detected leaving the ring, it is deleted from the OL accordingly.

Table 3-1: The OL Generation Process

Node ID	Address List of participating nodes								State	OL
A	A	F	B	-	G	D	E	A	*INRING*	AFBCDE
B	A	F	B	-	G	D	E	A	*INRING*	BGDEAF
C	A	F	B	-	-	-	-	-	*INRING->FREE*	-
D	A	F	B	-	G	D	E	A	*INRING*	DEAFBG
E	A	F	B	-	G	D	E	A	*INRING*	EAFBGD
F		F	B	-	G	D	E	A	*FREE->INRING*	FBCDEA
G					G	D	E	A	*FREE->INRING*	GDEAFB

Joining and Leaving Processes: As the vehicles running on the road are moving fast, nodes are joining nearby rings and leaving current rings frequently. So we are going to illustrate how the protocol deals with the joining and leaving situations.

The joining process is initiated by the token holder after data transmission if the node number does not reach to ring size. As example give in Fig. 3-4, four nodes A, B, C and D already form a ring with ring size 7 and the token holder now is A. A finishes the data transmission and since the node number is 4, so it sends OPEN token to accept new nodes into the ring and start a timer as T_{join}. Nodes 1, 2 and 3 hear the OPEN token and contend to send RM with their addresses to A. We assume nodes respond as the order: node 1, node 2 and node 3, so A updates OL by inserting their addresses between A and B. Once T_{join} expires, A sends the token to node 1 and node 1 builds its ring OL by the token information. Since the node number in OL already reaches ring size, there is no joining process initiated at node 1 after data transmission, therefore token is sent to node 2 according to OL. T_{join} is the sufficient time duration for a certain number of nodes joining the ring.

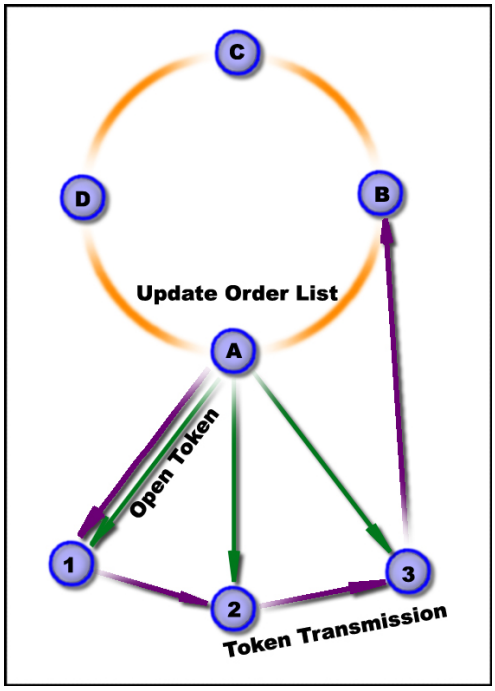

Figure 3-4: OTRP Joining Process

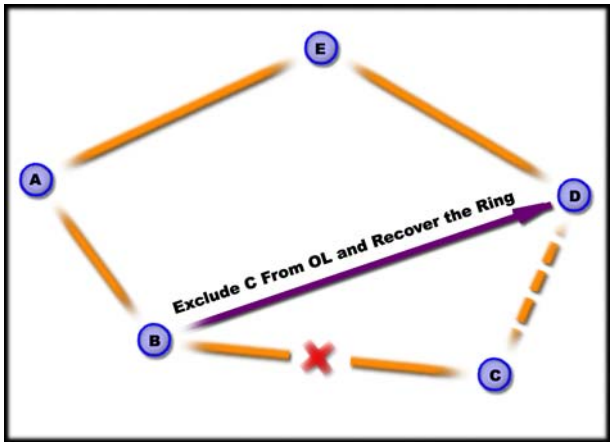

Figure 3-5: OTRP Leaving Process

Leaving process occurs when vehicles travel out of the token holder's radio range. The leave process is frequent due to the high mobility. When a token holder can not reach its next node by sending a token for *n* times, the next node is excluded from the OL and the toke holder tries to connect the next one in its OL. The status of the leaving node is set *FREE* when the timer for next token arrival expires and the timer is updated once a token transmission belonged to its ring is heard.

An example is given in Fig. 3-5. The node C is excluded from the ring when its previous node B can not reach it.

It is quite possible that the node holding the token leaves the ring during the time of its transmission. This can be detected when the node tries to pass the token to several different nodes but fails, i.e. the node leaves the dynamic cluster the ring resides so it can not find its next node. Under this circumstances, the host node will set itself status *FREE*. The ring then breaks and the nodes either wait to join other rings or initiate a new one as the initiation process described.

3.2.2 Emergency Mode

3.2.2.1 Description

The situation discussed above is by passing a token as the right to transmit. We are going to introduce the emergency mode to provide reliable broadcast with bounded delay.

Usually the emergency message should be broadcast as quickly and reliably as possible, but not as often as normal data service. In OTRP, the emergency message has the highest priority on transmission right, which means no matter there is a token on hand, it can be queued at the head of the buffer and broadcast once the node wins the medium contention. In order to guarantee the highest priority of the emergency message, special set of MAC parameters can be applied.

The token as the right for transmission is modified to ACK when the token holder receives the emergency message and. Then the token is passed as the OL, but different from the previous node, it no longer stays for data transmission. When the acknowledgement token reaches a node, it checks whether the emergency message has been received. If the result is positive, token ACK field will be tagged “yes”. Otherwise, if the node does not received the emergency message, the ACK token is modified to RQ and transmitted to its previous node. The previous node transmits the emergency message when it receives RQ and the ACK subsequently to acknowledge for the second time. The acknowledgement process stops when the token reaches a node whose message is already acknowledged, i.e., all the nodes in the ring have received the message. During the process, joining and leaving processes are also executed as the normal mode.

In the multiple overlapped rings situation, the acknowledgement processes are not synchronized, the data service will wait till not hearing any ACK token for a period of time. Fig. 3-6 shows the OTRP emergency mode.

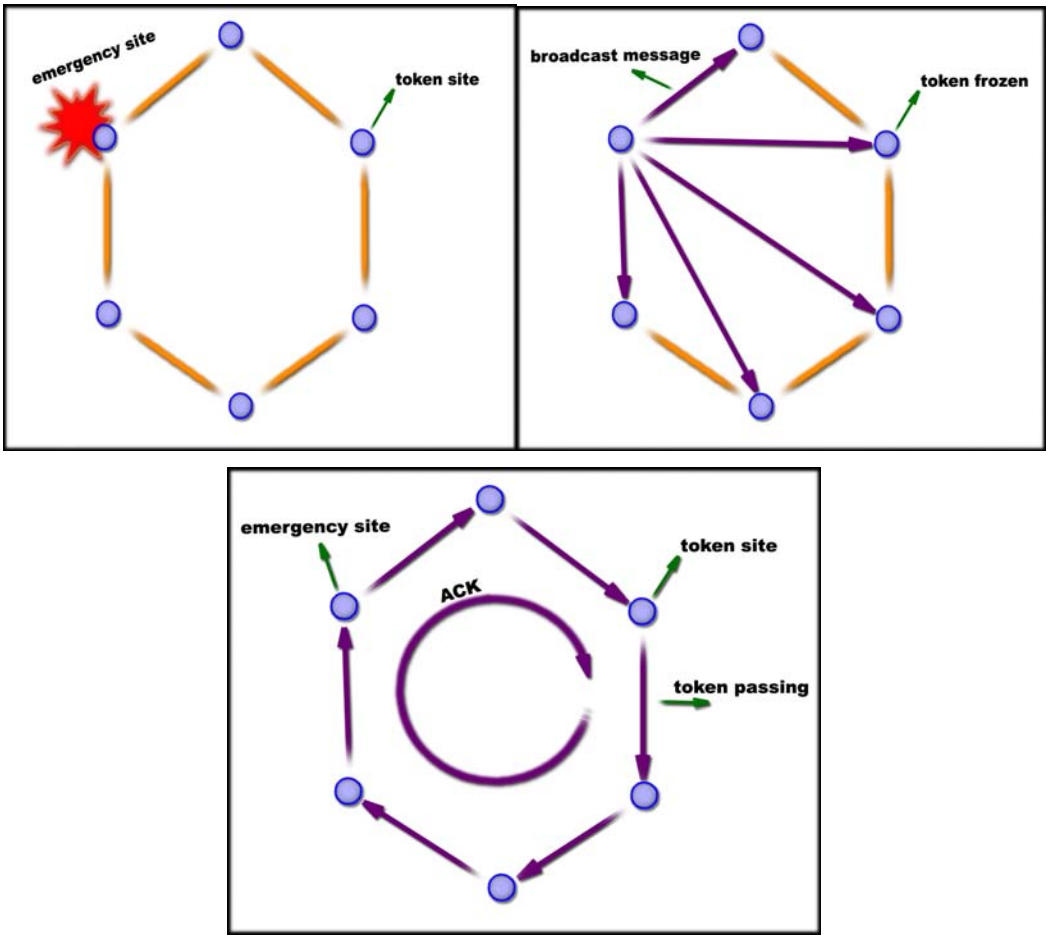

Figure 3-6: Emergency Mode in OTRP

3.2.2.2 Priority set for OTRP on IEEE 802.11 MAC layer

A priority scheme ensures the emergency node win the contention once the medium is idle. This can be achieved by setting special MAC parameters on the emergency node which depends on the under MAC layer. In this session, a priority scheme based on IEEE 802.11 MAC layer is explained.

We assume that when an emergency occurs at a node, a warning message is generated and waiting to be disseminated within short time. The back off counter for the emergency node is no long a uniformly distributed random number but is set to zero. At the same time, we assume in OTRP an extra delay is added to all the other nodes after the back off period. Therefore, once the channel is idle, the medium access delay for the emergency node is the shortest which guarantees its priority in transmission. Getting the right to transmit, the warning message is broadcast in a flooding way. Once

the token holder receives the warning message, the mode is switched from normal to emergency. The token holders then begin to acknowledge the warning messages in their own rings.

3.2.3 Ring Recovery Scheme

In vehicular environments, ring structure is dynamically adjusted. Several situations make ring structure unstable: failure to reach its next node; unable to transmit for *T_R* and the token holder itself leaves the ring. The approaches in OTRP dealing with these situations have been demonstrated in the former part. In a word, the protocol can recovers the ring structure from changing network topology in shot time.

The nodes' states are changing according to their locations and moving frequency. There are totally four states: *FREE*, *INRING_IDLE*, *INRING_BUSY* and *WAITING* in the normal mode as the state machinery transition presented in Fig. 3-7. The modes switching from data to emergency by hearing a broadcasted warning message and from emergency to data by the token holder does not hear any ACK token for a period of time.

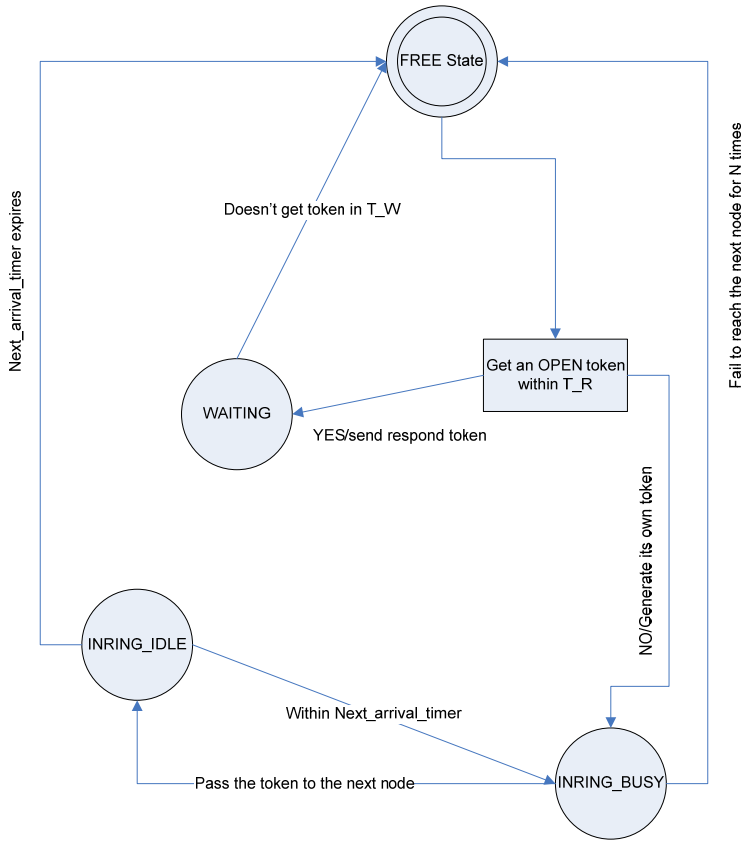

Figure 3-7: State Machinery Transition in Normal Mode

3.3 Conclusion

OTRP introduces a dynamical ring organization scheme to meet the requirements of IVC applications. It can formulate and sustain ring structures in a robust way which keeps the dominant transmission right by passing a token. Grouping vehicles in rings and assigning the right by passing a token can greatly decrease the collisions under dense traffic circumstances. The maximum time for data transmission at each node guarantees bounds the token rotation time and improves the fairness. Under emergency situations, the OTRP remedies the drawbacks of unreliable flooding broadcast by passing the token as an acknowledgement to the warning message.

The OTRP and WTRP are both inspired by the token ring concept which is originally used in the IEEE 802.4. The most noticeable difference between them is WTRP can not adapt to the vehicular environments and not suitable to a large number of nodes. Furthermore, it does not provide a reliable broadcast scheme for safety applications on IVC which is the core of vehicular communications.

Finally OTRP functions on MAC layer and only requires it supporting broadcast. Flexibility in choosing MAC layer protocol contributes to uncomplicated implementation.

Chapter 4 Performance Analysis

In this section, the performance of OTRP is evaluated by theoretical analysis. We study the network performance on a single ring mode with saturated traffic at first stage. The single ring's topology is affected by three sets of abstracted parameters: first is the traffic changing frequency which is reflected by vehicle's leaving probability. The second is the *FREE* node joining probability which is related to MAC contention scheme. The last is the OTRP parameters such as ring size and Maximum Token Holding time (*MTH*).

4.1 Network Model and Assumptions

In realistic situations, multiple rings exist concurrently in the same radio area and tokens should comply the contention scheme. In order to investigate the impact of related parameters to the performance of proposed OTRP, a single ring under network traffic saturated condition is considered.

The analysis is based on the following network model:

1) A dynamic communication area is considered. The traffic density is constant, i.e., the total number of vehicles in this area is certain. A typical communication area in realistic environments such as high way is defined by a certain length of the road with fixed number of lanes.
2) A ring is initially formulated with N nodes and the upper limit (ring size) is $N_{\max}$.
3) The dynamic network topology change is described by probability p_2 and *SLOT*. p_2 is the probability a node in ring leaving the area during a *SLOT*. Seen from a stationary view, the probability a node may leave the area is equal to the probability it may enter a new area. So p_2 represents the traffic changing rate within the specific area.
4) p_1 is the joining probability to the ring when a node in *FREE* state hears the OPEN token being sent out. The OPEN token is usually sent after a node finishes data transmission, provided the condition that the node number is less than $N_{\max}$.
5) The propagation and processing delay are usually very small thus can be ignored. But the transmission delay such as T_{TOKEN} (the token transmission time) is taken into consideration.
6) Traffic Model: the frame arrivals follow the Poisson distribution with parameter λ.

Table 4-1: Summary of Abstracted Parameters

Notations	Meaning	
p_1	Probability that *FREE* nodes can join the ring	Determined mostly by vehicles' traffic density and MAC scheme
p_2	Probability that a node leaves the communication area per *SLOT*	Reflects vehicle's moving rate
$N_{\max}$	Maximum node number in a ring	OTRP parameters
MTH	Maximum holding time for a token ring	
T_{TOKEN}	Transmitting time for a token	
λ	Frame arrival rate	Reflects network traffic condition

In performance analysis, by a *SLOT* of time, nodes can leave a ring and *FREE* status node can also join the ring under the condition that node number in the ring is unsaturated. Leaving and joining processes are independent.

We make following assumptions on parameters

1) All the control messages, i.e., tokens, are of the same size.
2) The duration that the token is passed from current token holder to the tagged station is denoted d_m and is measured by *SLOT*.
3) Traffic saturation condition is assumed which means there are always packets at a node's buffer to send when the token is on hand.
4) During each *SLOT*, at most a node leaves the ring.
5) When a joining process is initiated, there are always *FREE* nodes around.
6) Ignore the delay that is caused by MAC medium contention.

7) The “host node” is the node initiating join process. The “token holder” is the node currently holding the token.

8) New joining nodes obtain the token at least once.

9) The tagged node is assumed staying in the ring during analysis.

Table 4-1 summarise the network abstracted parameters relevant to performance analysis.

4.2 Performance Metrics

The performance of the proposed OTRP is evaluated using the following metrics.

1) Average access delay ($\overline{T_{AD}}$): the time interval between the moment a frame arrives the buffer and the moment it’s about to be sent.
2) Average throughput ($\overline{S}$): the average amount of payload per unit time the MAC layer delivers.
3) Average emergency delay ($\overline{T_{emer}}$): the interval between the moment the emergency message is generated and the moment when all nodes in *INRING* status within radio range have reliably received the messages, i.e. the messages have been acknowledged.
4) Average token rotation time **(**$\overline{T_{rotation}}$**)**: it is amount of time interval the token consecutively arrives at the same node.

4.3 Theoretical Analysis

In this section, the performance of OTRP in both data and safety applications is analyzed based on the proposed probability model. Performance metrics are presented by both constant and random abstracted parameters. Expectations are mathematically derived based on the assumptions given in last section.

4.3.1 Preliminary

The access delay consists of two parts as follows:

$W_{T,m}$: the duration the token is transmitted from token site to current node *m*.

$W_{Q,m}$: the delay that the frame waits in the queue before it’s ready to be sent. This can be derived by M/D/1 queue theory without considering the MAC layer delay. $W_{T,m}$ can be obtained as four parts:

current data transmission remaining time, time duration after token is released from current node to the tagged node get the token, time cost for join process and time cost for detecting leaving nodes.

$$W_{T,m} = T_R + (MTH + T_{TOKEN})(d_m - 1 + n_{adding} - n_{leaving}) + n_{init} \times T_{join} + n_{leaving} \times timeout \quad (4.1)$$

Joining and leaving processes are independent. T_{join} is the time duration sufficient for a certain number of nodes, say 3 in the analysis, to join the ring, this is a constant. The number of nodes joining the ring during each joining process has following distribution:

$$P(n = i) = \binom{3}{i} p_1^i (1 - p_1)^{3-i} \quad (4.2)$$

Similarly, since we assume the new join nodes can hold the token at least one time, during the process the number of leaving nodes follows distribution given in Equ. (4.3)

$$p(n = i) = \binom{d_m - 1}{i} p_2^i (1 - p_2)^{d_m - 1} \qquad i \in [0, d_m - 1] \quad (4.3)$$

timeout is a constant, signifying the time duration the host node needs to confirm the token has been successfully transmitted to the next node. Assuming a node transmits data once gets the token *timeout* can be estimated to T_{TOKEN} .

$$T_R = T_{TOKEN} + \frac{D_{remaining}}{R_{peak\_rate}} \quad (4.5)$$

$D_{remaining}$ is the remaining data in current token holder's buffer and R_{peak_rate} is the channel peak rate.

4.3.2 Average Access Delay ($\overline{T_{AD}}$)

d_m is uniformly distributed from 0 to N, thus $\overline{d_m} = E[d_m / N] = \frac{N}{2}$ (4.6)

For leaving nodes during the process:

$$\overline{n_{leaving}} = p_2 \times \overline{d_m} \quad (4.7)$$

The number of added nodes includes two parts. One is the initial unfilled positions, the other are those remedy leaving nodes. Equ.(4.8) represents the average number of joining nodes in total.

$$\overline{n_{adding}} = \left\lceil \frac{N_{\max} - N}{3} \right\rceil \times 3p_1 + \overline{n_{leaving}} \times p_1 \quad (4.8)$$

The number of joining processes generated during the process is $n_{init} = \left\lceil \frac{N_{\max} - N}{3} \right\rceil + \left\lceil \frac{\overline{n_{leaving}}}{3p_1} \right\rceil$ (4.9)

Regardless of the MAC layer contention delay, the time a frame needs to wait in the buffer is:

$$\overline{W_{Q,m}} = \frac{MTH}{2} \tag{4.10}$$

Equ. (4.10) can also represent the remaining transmission time of the token holder.

Summarize Equ. (4.1) to (4.10), the average access delay for the node is as follows:

$$\overline{T_{AD}} = (T_{TOKEN} + MTH)(\overline{d_m} + \overline{n_{adding}} - \overline{n_{leaving}}) + \overline{n_{init}} \times T_{join} + \overline{n_{leaving}} \times T_{TOKEN} \tag{4.11}$$

4.3.3 Average Token Rotation Time ($\overline{T_{rotation}}$)

To be specific, $\overline{T_{rotation}}$ can be referred to the time interval a node begins to send data and the next time the node gets the token.

$\overline{T_{rotation}}$ can be readily obtained after the ring is running into a stationary status under the assumption that there are always *FREE* nodes around. At this stage, the node number can reach to $N_{\max}$ at some time during a rotation cycle and d_m is considered as $N_{\max}$. The time cost for detecting leaving nodes and initiate joining process caused by leaving nodes are $N_{\max} \times p_2 \times T_{TOKEN}$ and $\left\lceil \frac{N_{\max} \times p_2}{3p_1} \right\rceil T_{join}$ respectively. Thus $\overline{T_{rotation}}$ can be calculated as:

$$\overline{T_{rotation}} = \left(MTH + T_{TOKEN}\right) \times (N_{\max} + N_{\max} \times p_1 \times p_2 - N_{\max} \times p_2) + \left\lceil \frac{N_{\max} \times p_2}{3p_1} \right\rceil T_{join} + N_{\max} \times p_2 \times T_{TOKEN}$$

(4.12)

4.3.4 Average Throughput ($\overline{S}$)

The average throughput is calculated from a node point of view. Since under saturated condition, each node has equal data transmission time. In stationary status that the node number keeps $N_{\max}$ most of the time, $\overline{S}$ can be obtained by dividing payload transmitted during one *MTH* over $\overline{T_{rotation}}$ as Equ. (4.13):

$$\overline{S} = \frac{MTH \times R_{peak\_rate} \times payload}{\overline{T_{rotation}} \times \left(payload + MAC + PHY\right)} \tag{4.13}$$

MAC and PHY are the MAC layer and Physical layer overhead respectively. Intuitively from the formula, $\overline{S}$ is decreasing by the increasing of $\overline{T_{rotation}}$. Thus additional processes, such as initial join process caused by leaving nodes, contributes to larger $\overline{T_{rotation}}$. And with larger $N_{\max}$, $\overline{S}$ is smaller due to increased $\overline{T_{rotation}}$. If in a radio range there is more than one ring, the number of nodes sharing the medium is increased which causes smaller $\overline{S}$.

4.3.5 Average Emergency Delay ($\overline{T_{emer}}$)

Emergency message is safety related to decrease the dangerous situations on road. Typical emergency message can be the traffic control message such as merging and splitting reminder, road condition indication as construction and bad weather warning and accident prevention warning such as rear-render collision avoidance. The feature of the emergency message is that it needs to be disseminated to effective range in short time with high reliability. However, the size of the message does not need to be long as it functions for situation awareness. Emergency delay is defined as the delay between the time an emergency message is generated to the time when *INRING* state nodes have reliably received the messages.

According to the emergency scheme discussed in Chapter 3, the emergency delay can be obtained as:

$$T_{emer} = T_{remaining} + T_{flooding} + \left(N - n_{leaving} + n_{adding}\right) \times T_{TOKEN} + n_{new} \times \left(2T_{token} + T_{message}\right) + n_{init} \times T_{join} + n_{leaving} \times timeout \quad (4.14)$$

In Equ.(4.14), n_{add_free} is the number of nodes that didn't receive the emergency messages. According to the network model, those are the number of nodes that join the ring after the message dissemination period. Based on the network assumption, n_{new} can be obtained as $n_{new} = n_{leaving} \times p_1$. $T_{flooding}$ is the broadcast duration. In analysis, $T_{flooding}$ can be considered as a constant that is the time an emergency message needs to reach the farthest node. $T_{remaining}$, on the other hand, is the delay an emergency message waits before it is broadcasted. The emergency event can possibly happen during the following periods: data transmission, token transmission, join process and the period token holder confirms a node left the ring. As indicated in Table 4-2, the $\overline{T_{remaining}}$ can be calculated by multiplying each probability with corresponding conditional expectation.

$$\overline{T_{emer}} = \overline{T_{remaining}} + T_{flooding} + (N - \overline{n_{leaving}} + \overline{n_{adding}}) \times T_{TOKEN} + \overline{n_{leaving}} \times p_1 \times \left(2T_{TOKEN} + T_{message}\right)$$
$$+ n_{init} \times T_{join} + \overline{n_{leaving}} \times T_{TOKEN} \quad (4.15)$$

If the ring is running into the stationary state described in 4.3.3, in which the node number is $N_{\max}$ most of the time, the acknowledgement token goes a rotation similarly as the data mode. Once message missing is discovered, the time cost for a retransmission is $2T_{token} + T_{message}$. Since the transmission time of a token is very short, so we assume the previous node will not leave beyond the radio range. The $\overline{T_{emer}}$ can be derived as Equ. (4.16), where $\overline{n_{leaving}}$ can be referred as $N_{\max} \times p_2$.

$$\overline{T_{emer}} = \overline{T_{remaining}} + T_{flooding} + (N_{\max} - \overline{n_{leaving}} + p_1 \times \overline{n_{leaving}}) \times T_{TOKEN} + \overline{n_{leaving}} \times p_1 \times \left(2T_{TOKEN} + T_{message}\right)$$
$$+ \left\lceil \frac{\overline{n_{leaving}}}{3p_1} \right\rceil \times T_{join} + \overline{n_{leaving}} \times T_{TOKEN} \quad (4.16)$$

Table 4-2: Expectations of Time Duration and Corresponding Probabilities for $\overline{T_{remaining}}$

Event name	Data transmission	Join Process	Detecting Leaving Process	Token Passing
Probability for each event	$\frac{MTH\left(N + \overline{n_{adding}} - \overline{n_{leaving}}\right)}{\overline{T_{rotation}}}$	$\frac{\overline{n_{init}} \times T_{join}}{\overline{T_{rotation}}}$	$\frac{\overline{n_{leaving}} \times timeout}{\overline{T_{rotation}}}$	$\frac{T_{TOKEN}\left(N + \overline{n_{adding}} - \overline{n_{leaving}}\right)}{\overline{T_{rotation}}}$
Conditional mean of $T_{remaining}$	$\overline{W_Q}$	$\frac{T_{join}}{2}$	$\frac{timeout}{2}$	$\frac{T_{token}}{2}$

The Equ. (4.16) is for a single ring situation. When multiple overlapped rings exist concurrently within same radio range, the acknowledge processes are not synchronized. Then the longest delay among the rings is the duration that nodes in the effective area reliably receive the emergency message, represented as $\overline{T_{emer}} = \max_i \left\{\overline{T_{i,emer}}\right\}$ (4.17)

where i is the identification of the ring.

4.4 Further Discussion

The analysis has focused on OTRP only which does not specify the MAC layer mechanism. The performance metrics impacted by ring size, join probability, leave probability and traffic situation are investigated. From the derived equations in section 4.3, we can see how three groups of parameters affect the performance.

First is the MAC layer channel access scheme. The MAC layer decides the right for which token to transmit when more than one ring are in the same range. Comparing to the common considerations of contention based MAC, the number of nodes involved in contention is smaller since within one ring, only a token has the right to transmit. Therefore, the number of collisions is greatly decreased. Furthermore, join probability is also related to MAC layer scheme, since there is contention between multiple *FREE* nodes during process.

Second is the network topology change or the vehicle's velocity. It is intuitive that the faster the speed, the harder to conduct a transmission and maintain the network topology stable. The leaving probability is the parameter representing the level of network topology change.

Finally is the impact of OTRP-specific parameters: the ring size, timeout for joining process, *MTH* and token size. There is a trade off in choosing the parameters. For instance, in terms of the ring size, since with larger ring size, token rotation time and access delay will be increased. Moreover with longer rotation time, nodes are more instable since the number of leaving nodes is related to ring size as Equ. (4.12). But on the other hand, medium contention is decreased under same traffic density, because larger ring size ends in less ring number.

To be more specific, from Equs.(4. 11), (4.12), (4.13) and (4.16), the $\overline{T_{AD}}$, $\overline{T_{emer}}$ and $\overline{T_{rotation}}$ alternate linearly with p_1 and p_2. But the joining nodes depends on p_2, since more nodes leave the ring, more joining processes are initiated, which means that p_2 has more influence than p_1 on network performance. In a single ring situation, it's obvious that longer $\overline{T_{rotation}}$ cause less throughput. This is intuitive, since $T_{rotation}$ is closely related to $N_{\max}$, more sharing nodes cause less throughput. The impact of $N_{\max}$ is significant, especially when *MTH* is large compared to T_{TOKEN} and T_{join} which may be the main parameter affecting $T_{rotation}$. Under the assumptions, it appears a linear relation to the time-related metrics. T_{TOKEN} and T_{join} are the overhead OTRP takes on the MAC layer,

therefore, the ratio of MTH over them also influences the efficiency of the ring protocol. While a larger ratio implies less protocol overhead but the access delay is also longer due to larger *MTH*. T_{join} is related the MAC channel access mechanism and the maximum number of nodes it can accept. So choosing suitable ring parameters for a specific traffic model is vital in obtaining good network performance.

4.5 Summary

This chapter provides the theoretical analysis of OTRP considering the dynamic change of ring topology and the effect of various MAC layer parameters. Saturated network traffic and dense vehicle environment are assumed. We obtain various important performance metrics, such as average frame access delay, average ring rotation time, average throughput of a node and the time for the emergency message delay that guarantees reliability.

Three sets of parameters affect the performance: the vehicles' probability and frequency moving into or out of an area, the MAC layer delay and the OTRP parameters. The parameters' impact on performance metrics from a theoretical view is given. From the analysis, carefully choosing OTRP parameters suitable for specific road traffic model is crucial in obtaining good network performance.

Chapter 5 Performance Evaluation

In this chapter, we evaluate the performance of the proposed protocol OTRP for vehicular networks using computer simulations. Firstly, the simulation model and parameters are described and explained. Secondly, numerical results are obtained and presented. Furthermore, simulation results are compared with theoretical results for verification, difference between them are explained. Finally, OTRP performance is analyzed and its advantages over vehicular communication networks are demonstrated.

5.1 Simulation Description

5.1.1 Simulation Model

The simulation is conducted by C language under Microsoft Visual Studio 2003 and it follows the same assumptions as those used in theoretical analysis for a fair comparison. Details are illustrated in section 4.1.

The simulator is designed to model the operation of OTRP with single ring. Each vehicle may be initiated with one of the statues: *FREE:* the vehicle is in the effective area but not belonged to the ring. *INRNG_IDLE:* the vehicle is in the ring without token on hand. *INRING_BUSY:* the vehicle is in the ring and holding the token. *EMPTY*: the vehicle is beyond the effective area. An existed ring is initiated when the simulation starts. The joining, ring recovery and reformation processes work as described in chapter 3. The propagation and processing delay are ignored. We assume that there is no transmission error and frame corruption at receiver side and nodes in the same radio range can always hear each other correctly.

Two scenarios are devised, one being the normal operation and the other representing the emergency situation. For the normal node, the operation is devised as event-driven. With *MTH* duration for data transmission and host node executes token pass according to OL information, essential joining or leaving processes are considered accordingly. Node's status is checked and changed by time frequency *SLOT*. For example, during each *SLOT,* an *INRING* node 4 is randomly chosen with a random probability generated, if the probability reaches p_2, status *EMPTY* is assigned to signify its leaving of the area. Otherwise it stays in the ring till next time chosen to be the changing node. Similar process is conducted per *SLOT* from *EMPTY* node to *FREE* to signify its entrance into

the area. Each time a node finishes *MTH* period, it checks the node number in OL If the node number is less than ring size; it sends out the OPEN token to accept new nodes. 3 *FREE* status nodes are randomly chosen each with a random probability. If the random probability reaches p_1, OL is updated and passed to the next node. In summary, a node's status changes either from *INRING* to *EMPTY* or *EMPTY* to *FREE* by *SLOT* and p_2, and switches between *INRING_IDLE* and *INRING_BUSY* by the token's residence. A node's status changes from *FREE* to *INRING* by the join process.

For the emergency situation, we set the emergency event to happen at 7000 ms which interrupts the normal mode. Two types of delay are defined as follows: T_{emer}, the interval between the time the warning message is generated to the end of acknowledgement. $T_{complete}$, the time interval that token begins to finishes acknowledgement. Each token transmission no matter in normal mode or emergency mode is recorded in a node's address list given its status is not *EMPTY*.

5.1.2 Simulation Parameters

We set MAC and PHY layer parameters as IEEE 802.11b standards with channel bandwidth 11Mbps. Frame payload is 500 bytes, MAC layer overhead 272 bits and PHY layer overhead 128 bits. The traffic comes to each node's buffer following Poisson process with average arrival rate λ. Each node can hold the token for *MTH* when the token arrives. Initially, there is a single ring with 3 nodes in it and 10 *FREE* nodes. We assume the total size of the nodes that have been defined statuses is 20.

Table 5-1: Simulation Parameters

TOKEN_SIZE	680+400 (MAC&PHY head) bits
MTH	200 ms
R_{peak_rate}	11Mbps
T_{join}	6 ms
SLOT	300 ms
MAX_SIZE	20
FRAM_SIZE	4400 bits
n_{per_join}	3

Abstracted network model described in chapter 4 is embodied with detailed process and specific parameters. The corresponding parameters to theoretical analysis are presented in Table 5-1. In particular, *MTH* is set 200 ms and token's payload is set 680 bits which is the payload size of all defined control tokens as well as the emergency message. Each format size in the token frame is defined in section 3.2.1. MAC and PHY layer overhead are set 400 bits as the standards. T_{join} is set 6 ms according to the access delay under severe MAC contention is 1ms under IEEE 802.11b, so 6 ms is enough for 3 node participation.

5.2 Numerical Results

We first investigate $\overline{T_{AD}}$'s changing trend with $N_{\max}$, p_1 and p_2. The $\overline{T_{AD}}$ here is the average delay the 3 initiated nodes obtain the token. In Fig. 5-1, we fix first p_2 as 0.2 and p_1 as 0.8 while vary the $N_{\max}$ from 4 to 9. The reason why ending at 9 is because large $N_{\max}$ causes long rotation time which is not recommended. In Fig. 5-2, $N_{\max}$ is fixed at 6 and p_2 as 0.2 and vary p_1 from 0.2 to 1. p_2's impact is also evaluated in Fig. 5-3 with $N_{\max}$ fixed at 6 and p_1 as 0.8 while vary p_2 from 0.1 to 1. Relevant explanations are given following the figures.

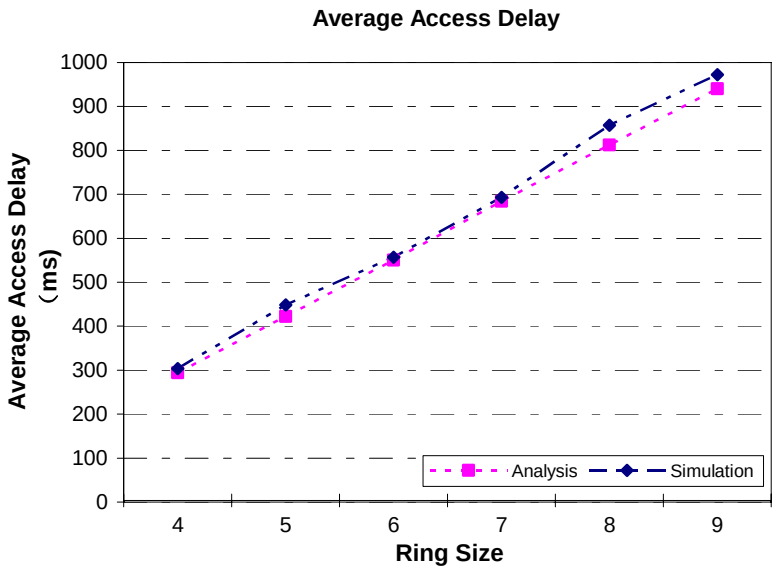

Figure 5-1: Average Access Delay vs. Ring Size

From Fig. 5-1, it can be seen that with the increase of $N_{\max}$, $\overline{T_{AD}}$ is increased linearly. This is because with larger $N_{\max}$, more nodes join through joining process. Under the assumption that a new joining node at least gets the token once and the time cost for the joining process and data transmission for each node is close, $\overline{T_{AD}}$ follows linear increase.

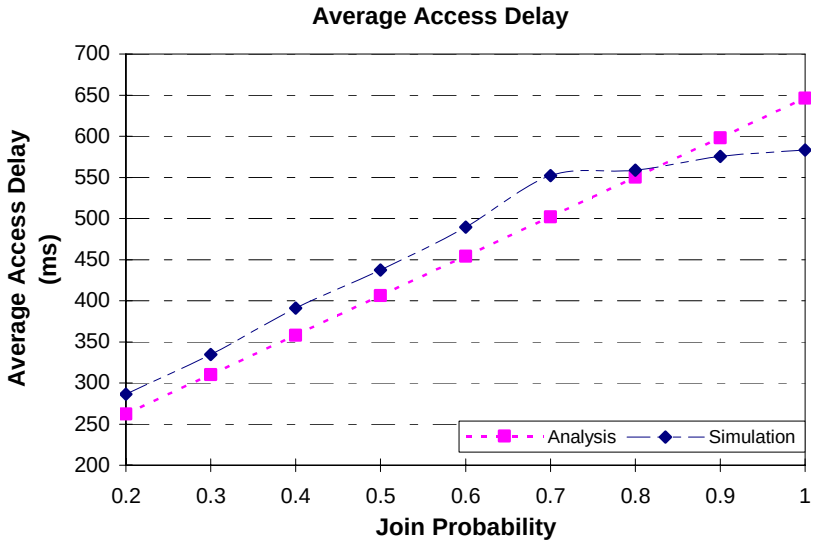

Figure 5-2: Average Access Delay vs. Join Probability

In Fig. 5-2, the join probability (p_1) has a significant effect to the $\overline{T_{AD}}$. Generally, with the increase of p_1, $\overline{T_{AD}}$ increases linearly. This is reasonable that by referring Equ. (4.11), $\overline{T_{AD}}$ has a approximated linear relation with p_1 since T_{join} is much smaller than *MTH*. However, when p_1 increases to 0.8 to 1, $\overline{T_{AD}}$ in the simulation increases moderately and appears a gap to theoretical analysis. The reason is that since nodes are more tend to join than leave the ring, the ring is more stable and easier to reach $N_{\max}$ which makes the access delay increase slowly. The gap between simulation and theoretical analysis is caused by the following reason. During the simulation, the node number is decided by checking current *INRING* status node number. While in the theoretical analysis, it's decided by OL, which is unaware of the nodes leaving after token is passed.

From Fig. 5-2 and Fig. 5-3, the leaving probability (p_2) has a minor effect on $\overline{T_{AD}}$, comparing to p_1. In Fig. 5-3, when p_1 is fixed at 0.8 and p_2 changes from 0.1 to 0.9, less than 10% difference occurs

in $\overline{T_{AD}}$'s value. $\overline{T_{AD}}$ is even slightly less when p_2 is high as fewer nodes keep *INRING* status makes the remaining quickly access the token. However, this is under the assumption regardless of the effects of MAC medium access delay. Intuitively, with high mobility, the chance a node access to medium will be reduced. As shown in these three figures, the analytical results agree well with the simulation results which validate the accuracy of our analytical model.

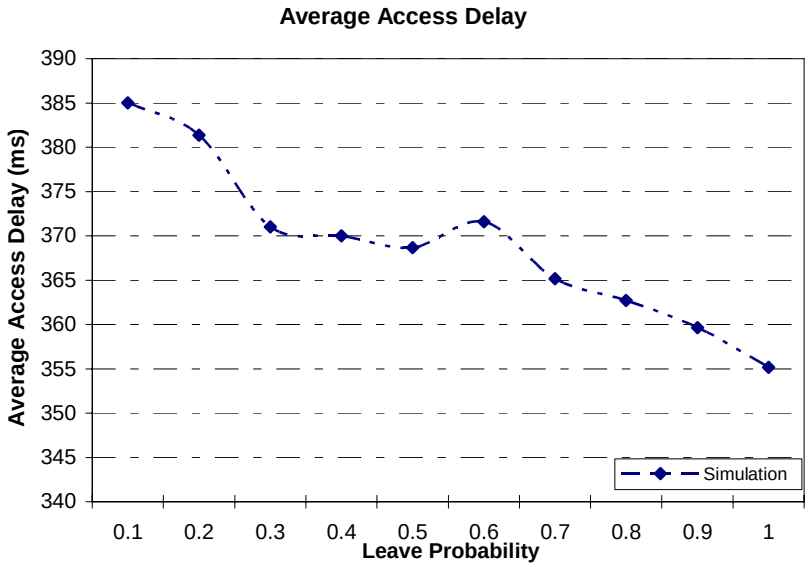

Figure 5-3: Average Access Delay vs. Leave Probability

Next, we study the average token rotation time ($\overline{T_{rotation}}$) under different ring size ($N_{\max}$) and join probability (p_1). Same parameter sets as $\overline{T_{AD}}$ are given. In Fig. 5-4, $\overline{T_{rotation}}$ follows a linear increase with $N_{\max}$. The amount for each increase is approximately a little more than 200 ms. This is reasonable since *MTH* is much larger compared to OTRP's overhead. Therefore, the time increased mostly depends on the additional data transmission time and the node number is the leading factor for this.

It can be seen from Fig 5-5, $\overline{T_{rotation}}$ appears a slow ramp increase vs. p_1 compared to $N_{\max}$. The theoretical analysis follows an approximated linear trend in accordance to Equ. (4.12), but for the simulation result, it shows a more gentle increase. The difference between the two can be explained as the reason given for $\overline{T_{AD}}$. The error is larger compared to $\overline{T_{AD}}$. This is because the token rotation lasts longer time that can cause more instability in topology change.

From Fig. 5-4 and Fig. 5-5, $N_{\max}$ shows dominant influence on $\overline{T_{rotation}}$ instead of p_1. However, this is under the assumption that the overhead is insignificant compared to data transmission. But this causes larger token rotation time and access delay. Thus, how to choose *MTH* value is important in obtaining optimized network performance.

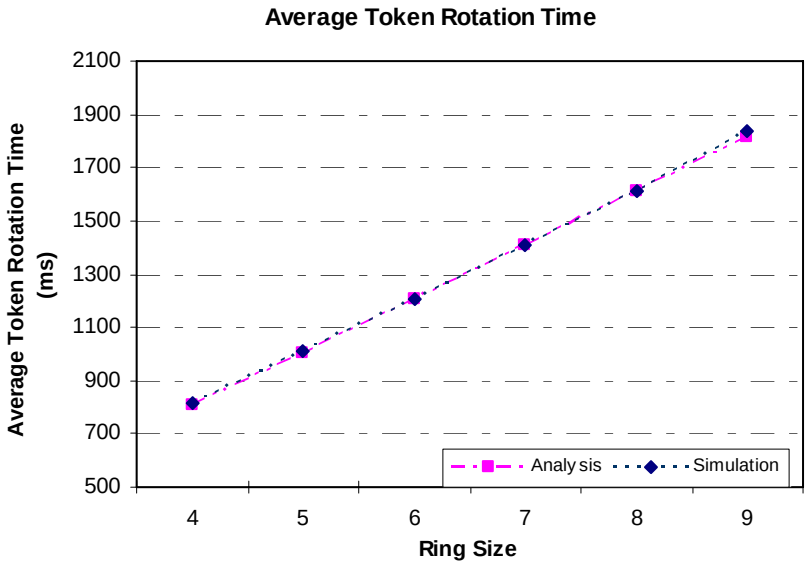

Figure 5-4: Average Token Rotation Time vs. Ring Size

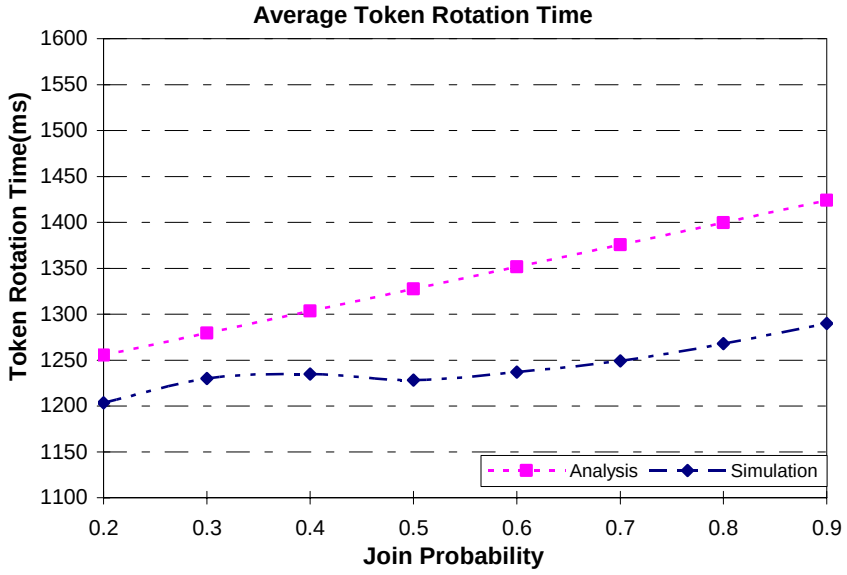

Figure 5-5: Average Token Rotation Time vs. Join Probability

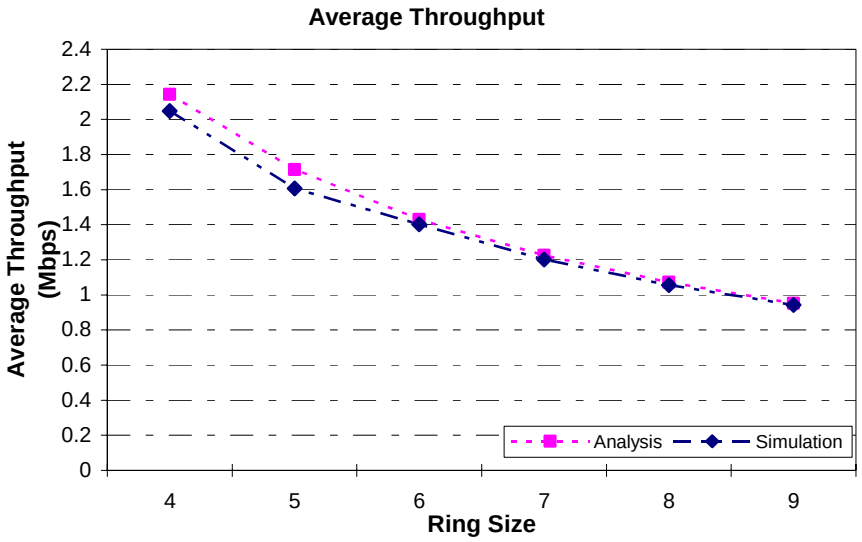

Figure 5-6: Average Throughput vs. Ring Size

Another important performance metric is the average per node throughput ($\overline{S}$). From Fig. 5-6, it can be seen that $\overline{S}$ changes with $N_{\max}$ in an inverse ratio. Intuitively, with more nodes sharing the medium, the throughput each node can gain is decreased. Furthermore, this can be explained given the previous result that $\overline{T_{rotation}}$ increases linearly with $N_{\max}$. By Equ.(4.13), $\overline{S}$ follows inverse ratio with $\overline{T_{rotation}}$.

Since OTRP introduces some overhead, the value of $\overline{S}$ depends on the ratio *MTH* over $\overline{T_{TOKEN}}$. If the ratio is set large, given same bandwidth, the value will be larger. In the analysis we set *MTH* 200 ms which is large compared to $\overline{T_{TOKEN}}$. From Fig. 5-6, we can see $\overline{S}$ is a little bit less than $\frac{R_{peak\_rate}}{N_{\max}}$, which shows high efficiency. But large *MTH* causes long $\overline{T_{rotation}}$ that delays the access to token. Therefore, *MTH* should be chosen wisely according to specific cases.

The average throughput per node ($\overline{S}$) versus p_1 is shown in Fig. 5-7. Under the assumption that nodes are densely populated, p_1 does not affect $\overline{S}$ much, especially when p_1 is large. When p_1 is from 0.3 to 0.9, $\overline{S}$'s reduction is within 5%. The simulation and analysis results are close with acceptable error.

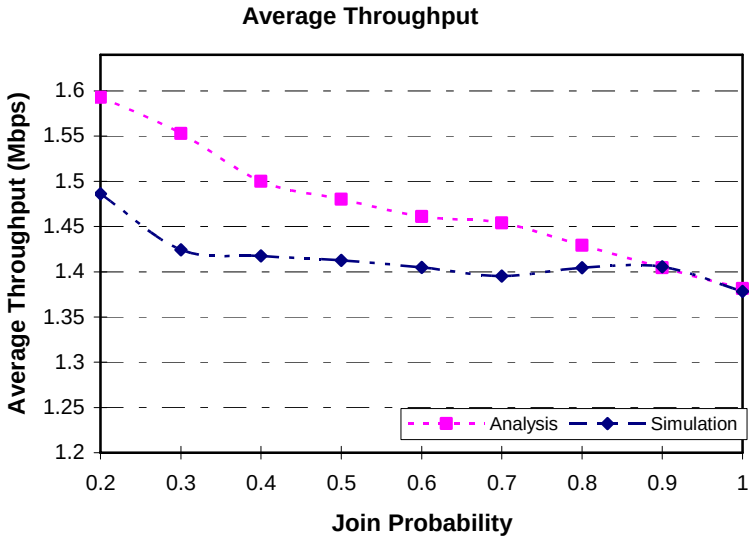

Figure 5-7: Average Throughput vs. Join Probability

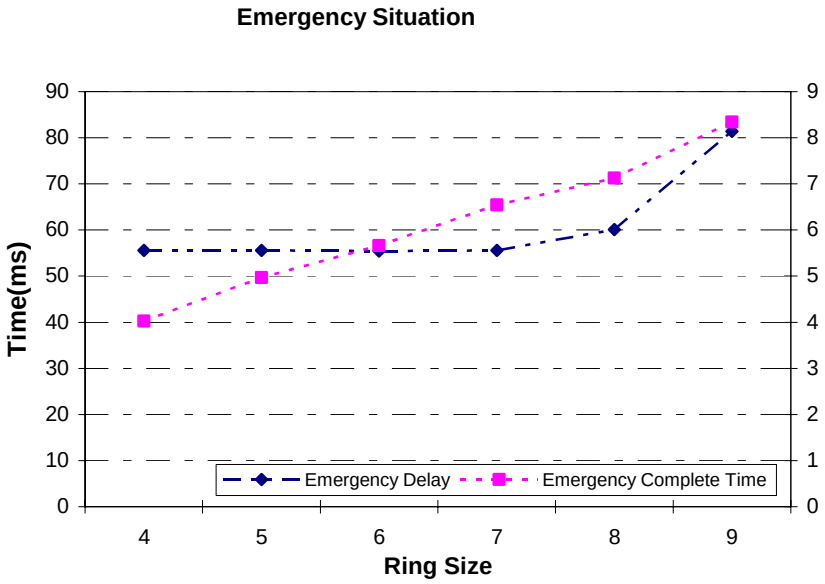

Figure 5-8: Average Emergency Delay and Complete Time changing vs. Ring Size

Fig. 5-8 and Fig. 5-9 present the impact of joining probability and ring size on two emergency mode metrics: average emergency delay ($\overline{T_{emer}}$) and average complete time ($\overline{T_{complete}}$). Emergency

complete time is the time cost in the moment warning message is sent to the time nodes in ring are acknowledged. In a 9 nodes size ring structure, $\overline{T_{complete}}$ is less than 10ms and $\overline{T_{emer}}$ is within 100ms which is very short. In Fig. 5-8, $\overline{T_{complete}}$ follows an approximated linear change versus $N_{\max}$, this can be referred to Equ. (4.16). Regarding $\overline{T_{emer}}$, because it includes the period of time emergency message waits before being broadcast, the increase is more gentle.

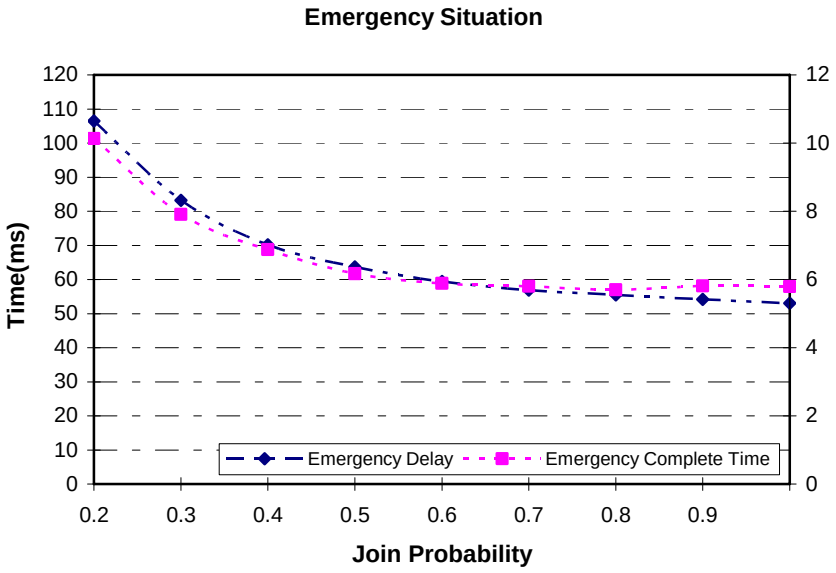

Figure 5-9: Average Emergency Delay and Complete Time vs. Join Probability

The $\overline{T_{complete}}$ changing trend that is shown in Fig. 5-8 and 5-9 however follows a gentle decrease versus p_1. This is because during emergency situation, nodes do not include any data passing process which makes $\overline{T_{complete}}$ no longer an approximated linear relation with p_1. Instead $\overline{T_{complete}}$ includes both a linear part and an inverse ratio part as:

$$\overline{n_{leaving}} \times p_1 \times \left(2T_{TOKEN} + T_{message}\right) + \left\lceil \frac{\overline{n_{leaving}}}{3p_1} \right\rceil \times \left(T_{join} + T_{TOKEN}\right) \tag{5.1}$$

And the trend Fig. 5-9 presents is reasonable as T_{join} is larger than T_{TOKEN}, which plays an important role on $\overline{T_{complete}}$'s gentle decrease in approximated inverse proportion versus p_1.

5.3 Further Discussion

From the numerical results, when *MTH* is set a large number compared to the T_{TOKEN} and T_{join}, for example 200 ms in the analysis, the overhead OTRP taken to MAC layer is released. Under this situation, $N_{\max}$ is significant in network performance rather than p_1 and p_2. But large $\overline{T_{rotation}}$ delays nods' access to token. On the contrary, if *MTH* is set small, for example as the extreme case in emergency situation which *MTH* is 0. The value set of T_{join} and T_{TOKEN} is important to network performance. p_1's effect is no longer approximated linear but consists an inverse ratio part as well. According to the numerical results p_2 does not affect the network performance severely in the evaluation of defined metrics. The principal reason accounted for this is that once nodes in rings are leaving, *FREE* nodes do not need to take long time to join the ring or form a new ring which shows that the OTRP is robust in recovering from quick losing nodes.

Bandwidth utilization is efficient according to the analysis of $\overline{S}$. And the advantage of the medium sharing scheme by passing a token is the fairness. Fig. 5-10 presents the simulation results of utilization efficiency within 1000s in the analyzed 20 nodes with $N_{\max}$ equal to 6. From Fig.5-10, the utilization efficiency is quite close to each other which prove good fairness of OTRP.

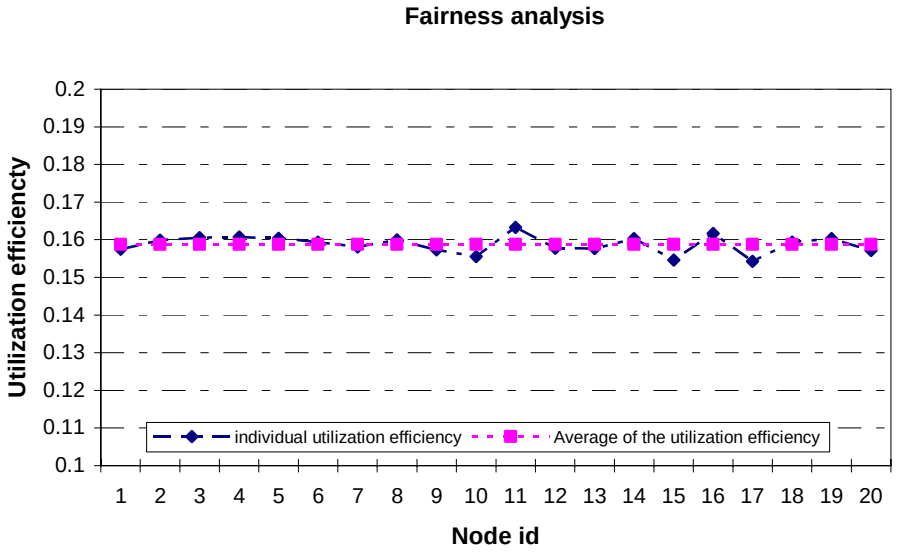

Figure 5-10: Fairness Evaluated by Utilization Efficiency

In the emergency situation, the acknowledgement rate, which is the acknowledged nodes over total number of nodes in the area, mainly depends on $N_{\max}$ and participation probability into a ring, i.e. the time proportion a node is in *INRING* status rather than *FREE* status. Generally, more involvement time in a ring contributes to high acknowledgement rate.

The values of $N_{\max}$ and *MTH* are flexibly chosen according to the environment to achieve optimized performance. For instance, there are 100 nodes in a 100 meters long high way and different combinations can be obtained given same MAC layer protocol. $N_{\max}$ determines the active node number involving the simultaneous contention as $\left\lceil \frac{100}{N_{\max}} \right\rceil$, and *MTH* affects the average token rotation time. In order to achieve promptly adjusting the ring structure, reducing the overhead OTRP has token and minimizing medium access carefully choosing OTRP parameter sets is crucial.

The theoretical analysis and the simulation results match each other well; the difference between them can be explained by in analysis the node number is checked by OL field in token format, while in simulation, it is checked by the number in *INRING* status which may have a quicker update.

5.4 Summary

In summary, simulations are conducted to evaluate both the accuracy of theoretical analysis and OTRP performance analysis. Numerical results are given regarding of the metrics defined in chapter 4 and presented in figures. Corresponding to the three groups of parameters mentioned in the last chapter, ring size has a significant effect on OTRP performance especially when *MTH* is set at large value. Besides, p_1's effect on $\overline{T_{rotation}}$ is approximately linear in normal mode while consists an inverse ratio part in the emergency situation. p_2 however has a minor impact comparing to other parameters.

$\overline{T_{AD}}$ and $\overline{T_{rotation}}$ show a predictable performance versus $N_{\max}$ and p_1. Average throughput is proven to be fair and high. In emergency situation, the time *INRING* nodes reliably receiving the message is very short which meets the requirements. OTRP shows its strong aspects in supporting transmissions under high mobile traffic conditions judged by p_2 as well.

Trade off in choosing parameter sets of OTRP are explained and to specific situations, suitable parameters have an important effect in obtaining good performance.

Chapter 6 Conclusion and Future Work

In this thesis, an overlay token ring protocol (OTRP) for vehicular communication networks has been proposed that works on top of MAC layer. It aims to solve the frequently changing network topology challenge of vehicular networks and provide QoS to both data and safety applications.

Several schemes are devised in OTRP to achieve the onjectives. Firstly, it applies tokens as control messages to organize and maintain ring structures in vehicular environments. Secondly, adaptive joining, leaving and reformulation schemes keep dynamic ring structure adjusted according to vehicles' movement. Smart management in ring order list and interaction between overlapped rings contributes to awareness of current neighbouring nodes as well.

The main advantages of this protocol are it greatly improves the fairness and bounds access delay by limiting the time for each transmission after getting the token. Contentions are reduced especially when traffic is dense since each ring has only one node involved in medium contention. The highest priority for warning message and token acknowledgement scheme provide a reliable and prompt broadcast way for safety applications.

The performance for saturated traffic and single ring situation is analyzed based on the probability model. Simulations results verify the analysis and demonstrate high and fair throughput for data transmission even when the traffic is in high mobility. The numerical results also show the delay for nodes in the communication area to reliably receive the warning message is short, which is within 0.1 second. Furthermore, there is a trade off in choosing OTRP parameters. For instance, under the assumption of same traffic density, the smaller the ring size, the severe contentions occur. But shorter token rotation time provides quicker access to medium and more flexible ring structure adjustment. The chosen of the overlay ring protocol parameters depends on specific traffic conditions and applications.

The proposed OTRP is at rudimentary level which needs more refinements. Three aspects are planed in future research.

1) More accurate analysis based on specific MAC layer and practical traffic model is a must stage.

2) Situation of overlapped rings and interaction between rings such as message relay should be a potential research topic.

3) Predefined vehicular application requirements can be tested by applying OTRP to evaluate its feasibility in real models.

Other considerations regarding of the algorithms in reducing overlay overhead and optimized parameter settings should be explored further to make the overlay token ring protocol specification complete.

Abbreviations and Symbols

Abbreviations:

ACK	Acknowledgement
BCH	Basic Channel
CDMA	Code Division Multiple Access
CSMA/CA	Carrier Sense Multiple Access/ Collision Avoidance
CTS	Clear to send
DCF	Distributed Coordination Function
DSRC	Dedicated Short Range Communications
EDCA	Enhanced Distributed Channel Access
FI	Frame Information
GPS	Global Positioning System
GSM	Global System for Mobile communications
IVC	Inter-Vehicle Communication
MAC	Medium Access Control
MANETs	Mobile Ad-hoc Networks
M-RBP	Mobile- Reliable Broadcast Protocol
MTH	Maximum Token Holding time
MTRT	Maximum Token Rotation Time
NoN	Number of Node
OL	Order List
OTRP	Overlay Token Ring Protocol
QoS	Quality of Service
PATH	Partners for Advanced Transit and Highways
PREVENT	The Integrated Project PReVENT is a European automotive industry activity co-funded by the European Commission to contribute to road safety by developing and demonstrating preventive safety applications and technologies
RBP	Reliable Broadcast Protocol
RNP	Reliable Neighbouring-cast Protocol

RTS	Ready to send
RVC	Road-to-Vehicle Communication
TDMA	Time Division Multiple Access
TDD	Time Division Duplex
T-RMP	Time-driven Reliable Multicast Protocol
VANETs	Vehicular Ad-hoc Networks
WILLWARN	Wireless Local Danger Warning
WTRP	Wireless Token Ring Protocol
WAVE	Wireless Access in Vehicular Environments

Symbols:

T_{AD} : Access delay

$T_{rotation}$: Token rotation time

T_{emer} : Emergency message dissemination delay

$T_{complete}$: Emergency complete time

$\overline{S}$: Average throughput per node

$N_{\max}$: Maximum ring size

p_1 : Probability a *FREE* node can join an unsaturated ring

p_2 : Probability a node leaves a ring

T_{TOKEN} : Token transmission time

timeout : Time bound confirming a token is lost during transmission

n_{add_new} : The number of nodes joining the area after emergency message dissemination period

n_{per_join} : The maximum number of nodes a join process can accept

$T_{remaining}$: Time a safety message wait for transmitting

$T_{flooding}$: Time to broadcast the safety message

R_{peak_rate} : Maximum channel rate

N : The number of nodes that are already in the ring

Bibliography

[1] F. Borgonovo, A. Capone, M. Cesana, and L. Fratta, "ADHOC MAC: New MAC Architecture for Ad Hoc Networks Providing Efficient and Reliable Point-to-Point and Broadcast Services," Wireless Networks, vol.10, July 2004.

[2] J. Luo and J. P. Hubaux, "A Survey of Inter-Vehicular Communication," Technical Report IC/2004/24.

[3] H. Menouar, F. Filali, and M. Lenardi, "A survey and qualitative analysis of MAC protocols for vehicular ad hoc networks," IEEE Wireless Communications, vol. 13, no. 5, pp: 30-35, October 2006.

[4] N. Maxemchuk, "Reliable multicast with guaranteed delay," IEEE Communications Magazine, vol. 40, no. 9, pp. 96- 102, September 2002.

[5] TL. Willke and N. Maxemchuk, "Reliable collaborative decision making in mobile ad hoc networks," in Proc. 7th IFIP/IEEE Int. Conf. MMNS, 2004.

[6] D. Lee, R. Attias, A. Puri, R. Sengupta, S. Tripakis, and P.Varaiya, "A wireless token ring protocol for intelligent transportation systems," in Proc. of IEEE Intelligent Transportation, pp. 1152-1157, 2001.

[7] M. Ergen, D. Lee, R. Sengupta, and P. Varaiya, "Wireless token ring protocol," IEEE Transactions on Vehicular Technology, vol. 53, no. 6, pp.1863- 1881, November 2004.

[8] Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements- Part 11: Wireless LAN Medium Access Control and Physical Layer Specifications- ANSI/IEEE Std. 802.11, 1999 Edition (R2003).

[9] X. Lu, G. Fan, and R. Hao, “A dynamic token passing MAC protocol for mobile ad hoc networks,” in Proc. of the 2006 international conference on Communications and mobile computing, pp. 743-748.

[10] W. Chen and S. Cai, “Ad hoc peer-to-peer network architecture for vehicle safety communications,” IEEE Communications Magazine, vol. 43, pp.100- 107, April 2005.

[11] N. Malpani, Y. Chen, NH. Vaidya, and JL. Welch “Distributed token circulating on in Mobile Ad-hoc networks,” IEEE Transactions on Mobile Computing, vol. 4, no.2, pp.154-165, March 2005.

[12] T. Hasegawa, K. Mizui, H. Fuji and K. Seki, “A concept reference model for inter-vehicle communications (report 2),” In Proc. of Intelligent Transportation Systems, the 7th International IEEE Conference, pp. 810- 815, October 2004.

[13] S. Biswas, R. Tatchikou, and F. Dion, “Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety,” IEEE Communications Magazine, vol.44, no.1, pp.74-82, January 2006.

[14] “Evaluation of a multi-channel protocol for multi-hop inter-vehicle Communications in road traffic environment,” Toyota Info Technology center co. Ltd , July 2005.

[15] C. J. Merlin and W. B. Heinzelman, “A study of safety applications in vehicular networks,” IEEE International Conference on Mobile Ad hoc and Sensor System Conference, pp.8, November 2005.

[16] M. Ergen, D. Lee, R. Sengupta, and P. Varaiya “Wireless token ring protocol-performance comparison with IEEE 802.11 - Computers and Communication,” in Proc. of ISCC 2003, vol. 2, pp. 710- 715, July 2003.

[17] Z. Deng, Y. Lu, C. Wang, and W. Wang, “EWTRP: enhanced wireless token ring protocol for small-scale wireless ad hoc networks,” ICCCAS 2004, vol. 1, pp. 398- 401, June 2004.

[18] C.-C. Lim, L. Yao, and W. Zhao, "A comparative study of three token ring protocols for real time communication," IEEE 11th International Conference on Distributed Computing System, pp.308-31, May 1991.

[19] O. Tickoo and B. Sikdar, "Queueing analysis and delay mitigation in IEEE 802.11 random access MAC based wireless networks," IEEE INFOCOM 2004, vol.2, pp.1404- 1413, March 2004.

[20] A. Nasipuri, S. Ye, J. You, and R.E. Hiromoto, "A MAC protocol for mobile ad hoc networks using directional antennas," IEEE Wireless Communications and Networking Conference (WCNC) 2000, vol.3, pp. 1214-1219, September 2000.

[21] Y. Ko, V. Shankarkumar, and N.H. Vaidya, "Medium access control protocols using directional antennas in ad hoc networks," IEEE INFOCOM 2000, vol.1, pp. 13-21, March 2000.

[22] J. Chand and N.F. Maxemchuk, "Reliable broadcast protocol," ACM Transactions on Computer Systems (TOCS), vol. 2, no. 3, pp. 251-273, August 1984.

[23] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function Performance analysis of the IEEE 802.11 distributed coordination function," IEEE Journal on Selected Areas in Communications, vol. 18, pp. 535-547, March 2000.

[24] H. Hsieh and R. Sivakumar, **"**IEEE 802.11 over multi-hop wireless networks: problems and new perspectives," in Proc. of Vehicular Technology Conference 2002, vol. 2, pp.748- 752, fall 2002.

[25] J. Jun and M.L. Sichitiu, "Fairness and QoS in multi-hop wireless networks," Vehicular Technology Conference, 2003, vol. 3, pp. 2936- 2940, fall 2003.

[26] Q. Xu, T. Mak, J. Ko, and R. Sengupta, “MAC protocol design for vehicle safety communications in dedicated short range communications spectrum,” in Proc. of IEEE ITSC, http://path.berkeley.edu/dsrc/pub/ITSC04.pdf, 2004.

[27] F. Borgonovo, L. Campelli, M. Cesana, and L. Coletti, “MAC for ad hoc inter-vehicle network: service and performance,” IEEE Vehicular Technology Conference 2003, vol. 5, pp. 2789-2793, fall 2003.

[28] H.W. So and J. Walrand, “McMAC: A multi-channel MAC proposal for Ad-Hoc wireless networks” http://www.cs.berkeley.edu/~so/pubs/mcmac_desc.pdf.

[29] Z. Deng, Y. Lu, C. Wang, and W. Wang, “E 2 WTRP: An energy-efficient wireless token ring protocol,” IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2004 (PIMRC 2004), vol.1, pp. 574- 578, September 2004.

[30] D. Lee, M. Ergen, R. Sengupta, and P. Varaiya, “Wireless token ring protocol for ad-hoc networks,” in Proc. of IEEE Aerospace Conference 2002, vol. 3, pp. 1219-1228.

[31] R. Baldessari, A. Festag, A. Matos, J. Santos, and R. Aguiar, “Flexible connectivity management in vehicular communication networks,” in Proc. of 3rd International Workshop on Intelligent Transportation, pp. 211-216, March 2006.

[32] S. Sheu, Y. Tsai, and J. Chen, “A highly reliable broadcast scheme for IEEE 802.11 multi-hop ad hoc networks,” IEEE International Conference on Communications 2002, vol.1, pp. 610-615.

[33] X. Ling, L. X. Cai, J. W. Mark and X. Shen, “Performance analysis of IEEE 802.11 DCF with Heterogeneous Traffic,” in Proc. of CCNC’07, pp.49-53, January 2007.

[34] T.L. Willke and N.F. Maxemchuk, “Reliable collaborative decision making in mobile Ad Hoc networks,” in Proc. of 7th IFIP/IEEE Int. Conf. MMNS 2004, vol. 3271/2004, pp. 88-101.

[35] “Mobile Ad hoc Networks” http://en.wikipedia.org/wiki/Mobile_ad-hoc_network.

[36] http://www.dalewright.net/category/telecommunications/wireless/wifi/

[37] P. Top, V. Kohlhepp, and F. Dowla, “A Token Ring Protocol for Dynamic Ad-hoc Wireless Environments,” Presented at: LLNL Internship Program, pp. 734-748, September 2005.

[38] E.E. Johnson, Z. Tang, M. Balakrishnan, J. Rubio, H. Zhang, and S. Sreepuram, “Robust token management for unreliable networks,” IEEE Military Communications Conference, 2003, vol.1, pp. 399- 404, October 2003.

[39] Y. Choi, B. Kim, K. Jung, H. Cho, and S.H. Kim, “An overlay multicast mechanism using single-hop clustering and tree division for mobile ad-hoc networks,” IEEE Vehicular Technology Conference 2006, pp. 921- 926, spring 2006.

[40] http://www.sevecom.org/Presentations/2006-11_Berlin/Sevecom_2006-11-15_D%20C2C_PhyMacNet.pdf

[41] W. Hou, W. Liu, and M. Fei, “A token-based MAC oriented wireless industrial control networks,” IEEE International Conference on Information Acquisition 2006, pp. 22-25. August 2006.

[42] CF. Chiasserini, E. Fasolo, R. Furiato, and R. Gaeta, “Smart broadcast of warning messages in vehicular ad hoc networks,” Workshop Interno Progetto NEWCOM (NoE), 2005.

[43] Y. Zang, L. Stibor, GR. Hiertz, and HJ. Reumerman, “Vehicular wireless media network (VWMN): a distributed broadband MAC for inter-vehicle communications,” in Proc. of the 2nd ACM international workshop on Vehicular ad hoc networks 2005, pp. 95-96.

[44] Y. Zang, L. Stibor, B. Walke, HJ. Reumerman and A. Barroso, “Towards broadband vehicular Ad-Hoc networks- the vehicular mesh network (VMESH) MAC protocol,” in Proc. of IEEE Wireless Communications and Networking Conference 2007, pp.417-422, March 2007.

[45] P. Wang and W. Zhuang, “A token-based scheduling scheme for WLANs supporting voice/data traffic and its performance analysis,” IEEE Transactions on Wireless Communications, to appear.