Study on Enhancing Content Distribution in Vehicular Network

阿部, 海燕

(Degree)
博士（工学）

(Date of Degree)
2024-09-25

(Date of Publication)
2025-09-01

(Resource Type)
doctoral thesis

(Report Number)
甲第9019号

(URL)
https://hdl.handle.net/20.500.14094/0100492528

Doctoral Dissertation

Study on Enhancing Content Distribution in Vehicular Network

（移動体ネットワークにおけるコンテンツ配信の強化に関する研究 ）

July 2024

Graduate School of Engineering,
Kobe University

Kaien Abe
(Haiyan Tian)

Acknowledgements

This acknowledgement is dedicated to all those who have supported me in this thesis and life in Japan.

Time flies, and nine years of my Ph.D. journey have passed in the blink of an eye. Looking back on this period filled with challenges and achievements, I am deeply aware that the completion of this dissertation would not have been possible without the help and support of many professors, colleagues, and friends. With heartfelt gratitude, I would like to extend my sincerest thanks to them.

First and foremost, I would like to express my deepest gratitude to Professor Yoshiaki Shiraishi and Professor Masakatu Morii, for their meticulous guidance and unwavering support at every step of my academic research. Their profound knowledge, rigorous academic attitude, and passion for research have deeply influenced me, driving me to move forward on academic path. Their patience and encouragement have kept me going through difficult times, ultimately leading to the completion of this research.

During these years, I have had the fortune of meeting many outstanding professes, colleagues and classmates. I am grateful for the supervise and support in academic vision, research projects and campus life, special thanks to Professor Seiichi Ozawa, Professor Masahiko Saito, and classmate Dr. Keisuke Furumoto.

Finally, I want to thank my family, bosom friends and colleagues in China and Japan for their selfless help, support and understanding. There is another special acknowledgement for them.

Words cannot express my gratitude. May we continue to achieve ideals in the future, facing new challenges and opportunities.

Abstract

Vehicular networks, facilitated by technologies, Dedicated Short Range Communications (DSRC) in Vehicular Environments, are essential for enhancing both safety and non-safety applications in Intelligent Transportation Systems. However, traditional TCP/IP-based content distribution faces challenges in complicated urban environments. Although there are no sufficient literatures to deeply explore this field, Content Centric Network (CCN) has shown significant foreground under the insight of merging CCN paradigms into vehicular networks. For achieving the merge, several challenges remain. Firstly, feasible strategies and schemes applied for vehicular network should be proposed and validated. Secondly, merging CCN into existing vehicular network standards like DSRC requires significant modifications. Additionally, high costs associated with deploying and maintaining infrastructures especially in densely populated urban areas, pose major bottleneck. Furthermore, due to existing research has not fully explored the potential of CCN for non-safety applications in vehicular networks, an effective simulation system for realistically and accurately evaluating has not yet been established. Besides, ensuring secure communication in highly dynamic and open environments necessitates robust cryptographic techniques. Though Identity-Based Encryption (IBE) is recognized as a better solution for vehicular networks comparing to Public Key Infrastructure, the key escrow issue is a bottleneck.

This dissertation addresses these challenges by proposing a comprehensive in-network caching framework for vehicular networks and leveraging DSRC to implement Vehicle-to-Vehicle (V2V) and RSU-to-Vehicle (R2V) communication which realizes CCN principle in practical applications. Additionally, this dissertation constructs an effective simulation platform by integrating well-known tools in network, vehicle traffic and road map fields. The integrated large-scale simulation platform represents a major leap forward vehicular network research. This more realistic and comprehensive simulation environment offers insights to researchers to develop, test, and refine network protocols and strategies with greater confidence and credibility. Furthermore, extensive simulations and performance metrics validate robustness against urban obstacles, reduction in RSU dependency, scalability, and reliability. Finally, this study reviews and compares various solutions to the IBE key escrow problem, ultimately selecting a practical solution for CCN-based vehicular networks. Considering the unique characteristics of dynamic nodes, including their strong mobility and timeliness, a PKG-Node distributed algorithm based on the principles of BF-IBE and D-PKG ideas is tailored. The algorithmic process is embedded into specific R2V and V2V scenarios. Moreover, a timeliness strategy for public keys based on vehicle identity IDs is integrated to mitigate key leakage risk for ensuring that compromised keys are only valid for a limited time.

By achieving these objectives, this research contributes a viable and superior alternative instead of traditional TCP/IP-based solutions for the development of content distribution mechanisms and security schemes in CCN vehicular networks. The findings of this study will provide valuable insights for future research and practical implementations in the field of intelligent transportation vehicular communication systems.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Research Background

Vehicular networks have emerged as a critical component of modern Intelligent Transportation Systems (ITS), supporting a wide range of applications from non-safety services to infotainment. These networks leverage communication technologies such as Dedicated-Short-Range-Communications (DSRC) and Wireless Access in Vehicular Environments (WAVE) to facilitate vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. DSRC, standardized globally, operates in the 5.9 GHz band and is designed to provide reliable, low-latency communication necessary for applications such as collision prevention, traffic management, and public safety services. Beyond safety applications, DSRC also supports non-safety applications, including internet access, multimedia content distribution, and various commercial services by traditional TCP/IP-based networking paradigm.

However, the traditional TCP/IP-based networking paradigm faces significant challenges in the context of vehicular networks, especially in urban environments. The dynamic and highly mobile nature of vehicles, coupled with obstacles such as buildings and other infrastructure, leads to intermittent connectivity and high data packet loss. These issues result in low data delivery ratios, particularly in dense urban areas where signal attenuation and radio frequency interference are prevalent. Additionally, the limited coverage range of DSRC and the high costs associated with deploying and maintaining Roadside Units (RSUs) further complicate the effective distribution of content in vehicular networks.

1.2 Current Research Status

To address the limitations of traditional TCP/IP-based solutions, researchers have explored alternative networking paradigms such as Information-Centric Networking (ICN) and Content-Centric Networking (CCN). ICN/CCN shifts the focus from host-to-host communication to content-centric communication, where data is accessed by its name rather than its location. This paradigm leverages in-network caching, where data is stored at various nodes within the network, thereby improving data availability, reducing latency, and enhancing network resilience.

In the context of vehicular networks, ICN/CCN has shown significant foreground and promise. ICN/CCN leverages in-network caching strategies, such as Leave Copy Everywhere

(LCE) and Least Recently Used (LRU), to address some of the fundamental limitations of TCP/IP-based solutions to enhance data availability and reliability in dynamically mobile vehicular environments of urban. LCE involves replicating content across multiple nodes to increase redundancy and availability, while LRU optimizes cache management by prioritizing frequently accessed content. Studies have demonstrated that these strategies can significantly improve content delivery metrics, including data delivery ratio and latency, compared to traditional TCP/IP-based approaches.

Despite these advancements, integrating ICN/CCN into existing vehicular network standards like DSRC presents several challenges. Maintaining cache consistency and efficient data dissemination in a highly dynamic and mobile environment is complex. Besides, the high costs and logistical challenges associated with deploying and maintaining RSUs, particularly in densely populated urban areas, remain significant bottlenecks. Moreover, there is limited research on its application for non-safety services, which are increasingly important as multimedia content and infotainment become more prevalent in vehicular networks. Additionally, maintaining stable, quantity, uninterrupted data dissemination in highly dynamic and mobile vehicular networks is complicated and difficult. The high costs associated with deploying and maintaining RSUs, especially in densely populated urban areas, pose another major bottleneck. Furthermore, due to existing research has not fully explored the potential of ICN/CCN for non-safety applications in vehicular networks, an effective simulation system for realistically and accurately evaluating has not yet been found.

1.3 Research Motivation

The motivation for this research arises from the need to overcome the limitations of traditional networking paradigms in vehicular networks and to explore the potential of ICN/CCN-based approaches to enhance content distribution. The primary motivations are as follows.

1.3.1 Improving Data Delivery in Urban Environments

As multimedia content and infotainment services become more prevalent, there is an increasing need to explore ICN/CCN-based approaches for non-safety applications in vehicular networks. Urban environments particularly pose significant challenges for vehicular communication due to high building density and frequent signal obstructions. Therefore, robust strategies are required to ensure high data delivery ratios and mitigate the adverse effects despite these challenges.

1.3.2 Reducing Dependence on Infrastructure

Deploying and maintaining RSUs is costly and logistically challenging. Developing strategies that minimize dependency on RSUs while ensuring efficient content dissemination is crucial. reduce reliance on fixed infrastructure by utilizing vehicle-to-vehicle (V2V) communication and in-network caching, thereby enhancing the flexibility and cost-effectiveness of vehicular networks.

1.3.3 Building an effective validation platform

Vehicular networks must handle varying traffic loads and dynamic mobility patterns. Ensuring that content distribution strategies scalable and reliable under different conditions is essential for real-world applicability. This research focuses on constructing an effective validation platform for testing and refining proposed strategies. Existing simulation tools for vehicular networks are fragmented, focusing separately on network simulation, vehicle traffic modeling, and map-based environmental contexts. This separation creates a gap in accurately representing the complexities of real-world vehicular communication environments. Given these limitations, there is a pressing need to develop an integrated simulation platform that combines these disparate elements into a cohesive whole. Such a platform would enable extensive simulations and performance analysis.

1.3.4 Exploring security measures for CCN vehicular network

Ensuring secure communication in highly dynamic and open environments necessitates robust cryptographic techniques. Though Identity-Based Encryption (IBE) is recognized as a better solution for vehicular networks comparing to Public Key Infrastructure, the key escrow

issue is a bottleneck. A solution that effectively distributes the key generation process between the PKG and individual vehicle nodes is needed. Additionally, for mitigating key leakage risks in CCN vehicular environment, a strategy that limits the utility of compromised keys should be discussed.

1.4 Contributions of the Dissertation

This dissertation addresses the challenges of traditional networking paradigms in vehicular networks by proposing and validating a comprehensive CCN-based in-network caching framework. The key contributions of this research are as follows:

1.4.1 Development of LCE In-Network Caching Strategy in vehicular networks

・Proposal and implementation of the Leave Copy Everywhere (LCE) in-network caching strategy tailored for vehicular networks. This strategy enhances content availability and delivery efficiency by leveraging vehicle mobility and dynamic caching.

・Design and integration of hierarchical naming structures and on-path routing mechanisms to improve data retrieval and routing efficiency in vehicular networks. These enhancements facilitate better content management and dissemination.

1.4.2 Leveraging of Content-Centric Networking in Dedicated Short-Range Communications in urban Environment

・Exploration and demonstration of leveraging Content-Centric Networking (CCN) with Dedicated Short−Range Communications (DSRC) for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. This research aims to optimize content distribution in urban environments characterized by high building density and frequent signal obstructions. The research includes the development of a protocol stack that coexists with both TCP/UDP/IPv6 for RSU-to-vehicle communication and CCN for V2V communication，and details a modified WAVE Service Advertisement (WSA) message to support CCN services for demonstrating the feasibility of implementing CCN in the DSRC framework.

1.4.3 Constructing Simulation Platform for credibility Validation in Realistic Deployments

・Proposal of large-scale simulation platform that represents a major leap forward in the field of vehicular network research. By providing a more realistic and comprehensive simulation environment, we empower researchers to develop, test, and refine network protocols and strategies with greater confidence and credibility. This advancement not only enhances the quality and applicability of research findings but also accelerates the development of robust and reliable intelligent transportation systems.

1.4.4 Exploring a solution for key escrow problem in CCN vehicular network

・Reviewing and comparing various solutions to the IBE key escrow problem, ultimately selecting a practical solution for CCN-based vehicular networks. Considering the unique characteristics of dynamic nodes, including their strong mobility and timeliness, a PKG-Node distributed algorithm based on the principles of BF-IBE and D-PKG ideas is tailored. The algorithmic process is embedded into specific R2V and V2V scenarios.

1.4.5 Integrating timeliness strategy for public keys based on vehicle ID

・Integrating a timeliness strategy for public keys based on vehicle identity ID into CCN vehicular network for mitigating key leakage risk. The proposed timeliness strategy ensures that compromised keys are only valid for a limited time.

1.5 Organization of the Dissertation

1.5.1 Chapter 2: LCE In-Network Caching on Vehicular Networks for Content Distribution

This chapter discusses the development and implementation of the Leave Copy Everywhere (LCE) in-network caching strategy. It details the methodology, simulation setup, and results, demonstrating the strategy's effectiveness in enhancing content distribution in urban vehicular networks.

1.5.2 Chapter 3: Leveraging In-Network Caching in Vehicular Network

This chapter expands on the application of in-network caching strategies in vehicular networks. It focuses on leveraging existing vehicular infrastructure and traffic patterns to optimize content dissemination. The chapter includes comprehensive simulations and analyses to validate the proposed approaches.

1.5.3 Chapter 4: CCN-Based Vehicle-to-Vehicle Communication in DSRC for Content Distribution in Urban Environments

This chapter explores the integration of Content-Centric Networking (CCN) with Dedicated Short-Range Communications (DSRC) for improving V2V communication. It presents the theoretical framework, practical implementation, and simulation-based validation, highlighting the benefits and challenges of this integration.

1.5.4 Chapter 5: A PKG-Node distributed Identity-Based Encryption scheme in CCN vehicular network

This chapter explores a solution for key escrow problem in CCN vehicular networks.

Considering the unique characteristics of dynamic nodes, including their strong mobility and timeliness, a PKG-Node distributed algorithm based on the principles of BF-IBE and D-PKG ideas is tailored for CCN vehicular networks. The algorithmic process is embedded into specific RSU-to-vehicle and vehicle-to-vehicle application scenarios. Additionally, a timeliness strategy for public keys based on vehicle identity IDs is integrated to mitigate key leakage risk. This approach assigns an expiration date to each public key, ensuring that compromised keys are only valid for a limited time.

1.5.5 Chapter 6: Conclusion and Future Work

This chapter summarizes the primary contributions of the dissertation, reflecting on the research's impact on enhancing content distribution in CCN vehicular networks. It also suggests potential areas for future research, aiming to further optimize and expand the proposed framework.

・Investigate the limitations of traditional TCP/IP-based content distribution in vehicular networks

・Develop a comprehensive in-network caching framework tailored for vehicular networks and evaluate it with vehicular environments

・Design a CCN-based V2V and V2I communication protocol leveraging DSRC in realistic application to enhance content dissemination in urban environments

・Constructing an effective real-time simulation platform by integrating well-known platforms of networks OMNeT++, vehicle traffics Veins and SUMO, road maps and other applications

・Performance Verification of the proposed schemes with conventional methods in various urban traffic scenarios

・Exploring a solution for key escrow problem and key leakage vulnerabilities in CCN vehicular networks by investigating current mainstream identity-based encryption algorithms

By achieving these objectives, this research contributes to the development of more efficient and reliable content distribution mechanisms in CCN vehicular networks. The findings of this study will provide valuable insights for future research and practical implementations in the field of intelligent transportation systems.

Chapter 2

LCE In-Network Caching on Vehicular Networks for Content Distribution in Urban Environments

2.1 Abstract

ICN/CCN advocates ubiquitous in-network caching to enhance content distribution. Non-safety application in vehicular communication is emerging beyond the initial safety application. However, it suffers from a typical issue of low delivery ratio in urban environments, where high buildings block and attenuate the radio propagation from RSU infrastructures as well as other technical issues. In this paper, LCE in-network caching strategy with LRU algorithm in vehicular networks is proposed according to traffic characteristics in metropolitan areas. We compare this scheme with the legacy TCP/IP based scheme by simulation tools of OMNeT++ & Veins and SUMO. The simulation results validate that the proposed scheme could achieve stronger robustness against obstacles, higher file capture rate and less dependency on RSU infrastructure.

2.2 Introduction

Information- or Content-Centric Network (ICN/CCN) has motived the development of future Internet architectures based on named data objects (NDOs), instead of the current internet of host-to-host communication model [1][2][3]. The common goal of ICN/CCN is to achieve efficient and reliable content distribution by providing a general platform for communication service that are today only available in dedicated system such as peer-to-peer (P2P) overlays and proprietary content distribution networks [1][2]. ICN/CCN leverages in-network caching to provide a better-performing and more robust transport service. In-network caching has emerged as a distinct research field in the context of ICN/CCN [4].

Non-safety application in vehicular communication is emerging beyond the initial safety application [5][6][7][8], underlying the trend that multimedia contents will represent more than 90% of the whole Internet traffics in a few years [9][10]. In-network caching applied in vehicular communication becomes a prospective direction despite currently the relative literatures on it is still limited yet. In this chapter, we will review the related research work and

propose LCE (leave copy everywhere) in-network caching scheme with LRU (least recently used) algorithm, which is applied to vehicular networks for proximity marketing distribution in a metropolitan area.

2.3 Related Works and Contribution

For vehicular communication, the automotive industry has standardized multiple radio and medium access technologies, e.g. DSRC (Dedicated Short-Range Communications,) and WAVE (Wireless Access in Vehicular Environments, IEEE 802.11p) for direct vehicle-to-vehicle communications (V2V) as well as vehicle-to-infrastructure communication (V2I) [6][7][11][12]. DSRC/WAVE can reach a transmission range of 100 to 500 meters, so that a vehicle travelling at normal speed can exchange at least 10 messages per second with 3K bits in each message [7]. Thus, it becomes foreseen on both safety and non-safety applications.

Based on TCP/IP and DSRC/WAVE standards, the literature in [6] indicates that coding techniques (coded storage) is effective for large files transmission over small files, and could speed up the download of large files in vehicular networks. The work in [8] tackled content downloading in vehicular networks by optimizing APs (access points) deployment, V2V relay and penetration rate. Above works are based on legacy TCP/IP solution. Although TCP/IP protocols have been proposed to run on top of DSRC/WAVE for data exchange among vehicles [7][11], a fundamental limitation is that the requirement of infrastructure support is needed for global IP address allocation [7], which is infeasible to assume a sustainable availability or dependency on infrastructure support due to instability connectivity with RSU infrastructures.

So far, few literatures of applying ICN/CCN to VANET (vehicular ad hoc networks) is exist, some examples being [5][7][11]. In [7], L.Wang et al. proposed named data and designed the data structure in vehicular communication. In [5], the proposed framework called IC NoW (Information-Centric Networking on Wheels) focus on the content and its scope of the information in space, time, and user interest. Literature in [11] opened the further design called CCVN (content-centric vehicular networking) and attempted on naming data, retrieval process as well as a preliminary evaluation, and concluded that consumers increasing.

Our work in this paper addresses an in-network caching strategy LCE (leave copy everywhere, i.e. every vehicle in the scenario can cache popular files) to VANET, and LRU (Least Recently Used) replacement algorithm runs in all caches. This scheme aims at content distribution of proximity marketing in a metropolitan area according to the characteristics of random and dynamic traffic in VANET. Every vehicle plays two roles as not only a subscriber to require files, but also an in-network cache for responding other vehicles interests and forwarding files to them. We will describe the details in Section III and IV.

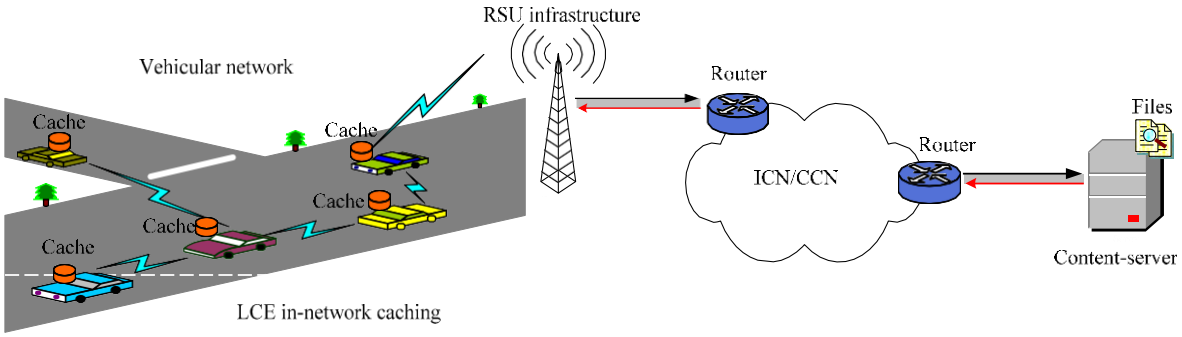

Fig. 2.1. LCE in-network caching-based content distribution scheme

Based on LCE in-network caching scheme, a serial of simulations in Section V are carried out by OMNeT++ & Veins framework in a real-world road traffic of an urban environment, which is accommodated by SUMO [13]. In the simulation, we compared the in-network caching-based scheme with the legacy solution of TCP/IP based scheme in several aspects:

2.3.1 Caching scheme and TCP/IP scheme

First, the impact of obstacles (e.g., buildings) is evaluated for two schemes by comparing their file capture rates. Proposed LCE caching scheme performs strong robustness and stability whether obstacles exist or not. In contrast, legacy TCP/IP based scheme is intensely influenced by obstacles.

2.3.2 Cache function

Secondly, the cache function is evaluated. We analyzed the file capture rate contributed by V2V transmission and by V2I transmission, respectively. The simulation results present that file capture rate achieved between caching nodes (V2V transmission.

2.3.3 Dependency on RSU

Moreover, we counted the broadcast frequency from RSU in both schemes, to evaluate the dependency on RSU. More broadcast frequency means the more requirement of downloading files via RSU, the more dependency on RSU. On the other hand, because RSU is connected with original content server for downloading files, RSU broadcast frequency is also an indirect evaluation on internet traffics. The simulation results indicate that the proposed scheme enables less broadcasts from RSU, thereby alleviates dependency on RSU infrastructure and decreases internet traffics.

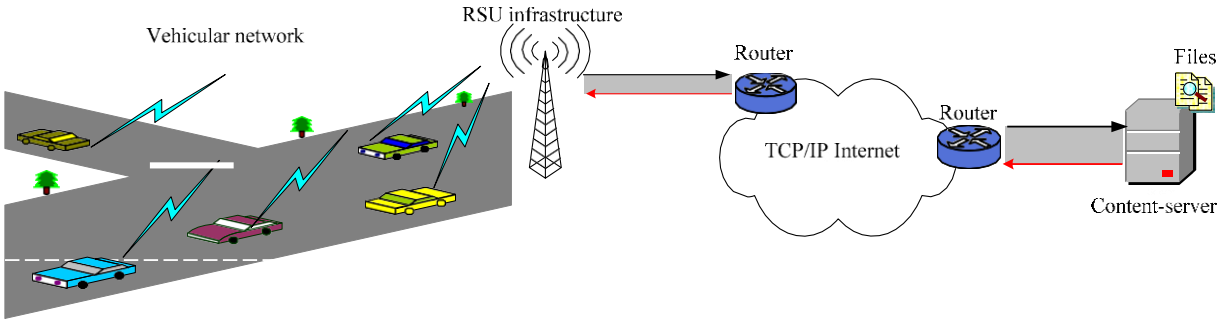

Fig. 2.2. TCP/IP based content distribution scheme

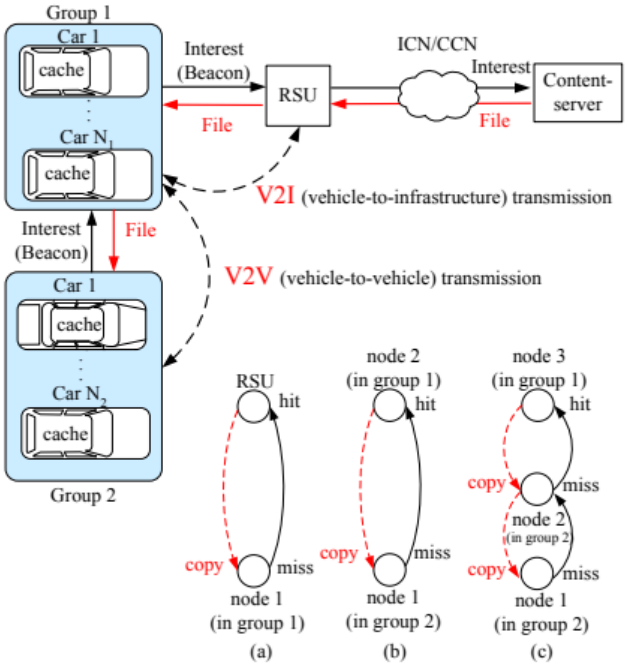

Fig. 2.3. LCE in-network caching-based file download

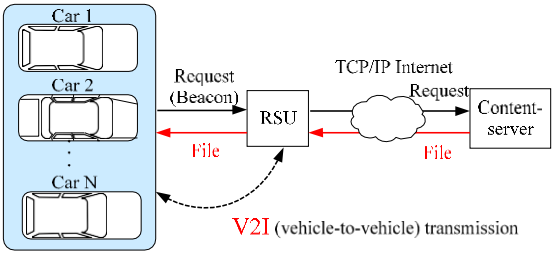

Fig. 2.4. TCP/IP based file download.

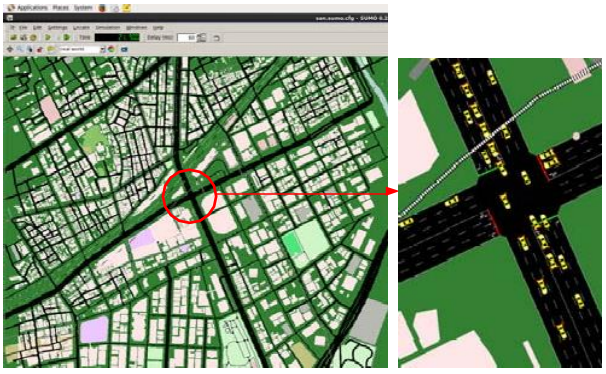

Fig. 2.5. A real-world road map produced by SUMO for simulation.

TABLE 2.1 Simulation parameters

Location	***Attitude:*** 34.6882~6978, ***Longitude:*** 135.1864~2017
Nodes	400 cars & 1 RSU
File	***Size:*** 1KB; ***File number:*** 100; ***Maximum files received by cars:*** 40000
Time	***Beacon interval:*** 1sec; ***Broadcast interval:*** 0.1 sec; ***Simulation time:*** 500 s; ***Duration of entering roads:*** 250 s

TABLE 2.2 Simulation results

Value	In-network caching based scheme	TCP/IP based scheme
Broadcast frequency from RSU	200/500 sec.	4798/500 sec.
Received files by V2I	999	27713
Received files by V2V	38735	--
Total received files	39734	27713

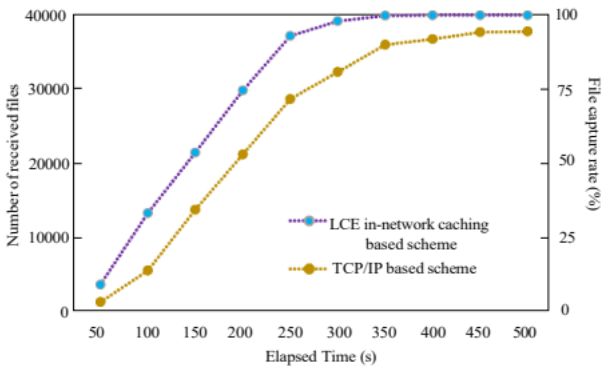

Fig. 2.6. Comparison between LCE in-network caching scheme and TCP/IP based scheme without obstacle module.

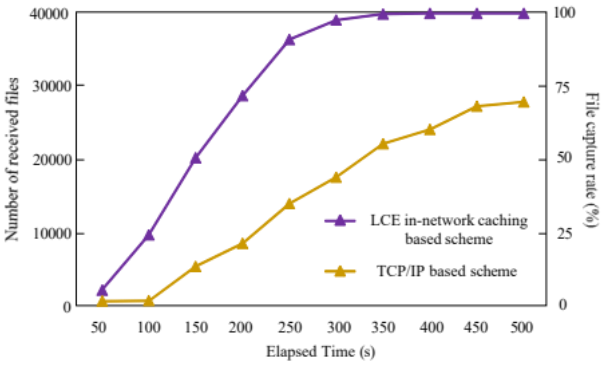

Fig. 2.7. Comparison between LCE in-network caching scheme and TCP/IP based scheme with obstacle module.

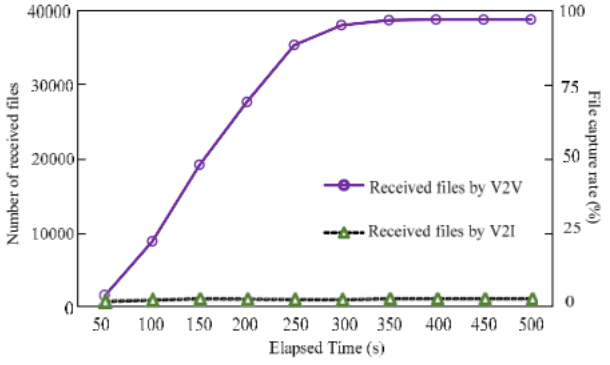

Fig. 2.8. File capture rates achieved by V2V and V2I transmission respectively in proposed scheme.

2.4 Comparison of LCE In-network Caching Schemes and TCP/IP Based Scheme in Vehicular Network

2.4.1 Our Proposal: LCE In-Network Caching based scheme

Content distribution in vehicular networks suffers from a typical issue: low data delivery ratio in urban environments, emitted where high buildings block and attenuate the radio propagation from RSU infrastructures [14][15]. On the other hand, other technical issues, e.g., absolutely necessary of connectivity with RSU for globe IP address allocation (aforementioned in section II), finite radio wave coverage range and limited APs deployment etc., cause a serious dependency on RSU infrastructures. Although more RSUs could be deployed to increase coverage rate of radio wave, it is deviated from the trend of reducing the resource of infrastructures and eliminating the network traffics. All of these issues are difficult to be tackled by legacy solution so that impel us to explore other solutions toward ICN/CCN paradigm.

Although there are sufficient cache strategy proposed for ICN/CCN in previous works, e.g., LCD (leave copy down), MCD (move copy down), Prob (copy with probability), Probe-Cache (a weighted probability cache) and so on [16][17][18][19], due to VANETs characteristic of mobility, short-lived and intermittent connectivity, caching strategy has to be uncoordinated and distributed, which is fit the random, dynamic and unstable features in V2V communication. Thereby in-network caching scheme called Leave Copy Everywhere (LCE) for every-vehicles are borrowed for V2V communication in our work. “Leave copy everywhere” can expand coverage range of transmission and decrease relay times. LCE in-network caching-based scheme for vehicle network is shown in Fig.1.

Besides, Least Recently Used (LRU) replacement algorithm runs in all caches. In a commercial region, proximity marketing files are most concerned. LRU algorithm in cache is reasonable according to link popularity. In this designed vehicular network, every vehicle plays two roles as not only a subscriber for requiring files, but also an in-network cache for responding other vehicles interests and forwarding files to them. The caches store high popular proximity marketing files and undertake data delivery instead of frequently connectivity with RSU infrastructure, so as to accelerate file transmission effectively and decrease the dependency on RSU.

In the vehicle network shown in Fig.1, as a first step, through V2I transmission, the content files are broadcasted to vehicles; a portion of vehicles receive files and possess these files as a content store. After that, files are directly delivered through V2V transmission to other vehicles, which relies on LCE in-network caching equipped in every vehicle. The cache stores epidemic files instead of RSU infrastructure. V2V transmission skips accessing content server, in some extent to accelerate file propagation.

2.4.2 Legacy solution: TCP/IP Based Scheme

In order to evaluate the performance of proposed scheme, a legacy solution of TCP/IP based scheme is shown in Fig.2 for comparison. In the legacy scheme, all of vehicles download files through V2I communication. Although file delivery sometimes happens through V2V relay, indeed the last relay node still needs a connection with infrastructures. In another word, all cars have to download files from RSU directly or indirectly. Because of this situation, we simplify file delivery route: assume all of vehicle download files from RSU infrastructure.

In this legacy solution, there are several problems difficult to be solved as well as the absolutely necessary of connection with RSU for globe IP address allocation. First, when all of vehicles download files from content-server via RSU, it causes crowded network traffics in the situation that currently internet bandwidth almost reaches the limit [6]. Besides, radio shadowing in urban environments derived from high buildings and other obstacles always cause unsuccessful access to RSU [14][15]. On the other hand, when a vehicle is quickly passing by an access point, it might not have sufficient time to accomplish a successful download. (However, it can be done from the vehicles that are driving on the parallel roads if these vehicles already possess requested files in their cache.)

2.5 Application Cases Description

Application cases corresponding to LCE in-network caching-based scheme and legacy TCP/IP based scheme are described in Fig.3 and 4 respectively. The target is all of cars capture and share in the same proximity marketing files that are initially placed in content server.

2.5.1 Case 1: for LCE in-network Caching Based Scheme

In the case of LCE in-network caching-based scheme shown in Fig.3, we sort cars into two groups. The cars downloading files from RSU (V2I) belong to Group 1. The cars downloading files from other cars (V2V) belong to Group2. The cache policy of Group1 shown in (a): after node 1 downloads file from RSU, caches this file. The cache policy of Group2 is shown in (b) and (c). The nodes in Group 2 download file by two ways. One is shown in (b): after node 1 download file from node 2 of Group1, caches this file. Another shown in (c) is, node 1 requests file via relay node 2 of Group2 to node 3 of Group1. On the back way, file is cached in every node. Above operations are repeated for every node until every node receives this file. In the simulation scenario of section V, 100 files and 400 nodes will act in accordance with this cache strategy.

Furthermore, in order to increase data delivery happened between cars (V2V) and reduce the dependency on RSU, we setup RSU broadcast as responding once per 10 beacon requests.

2.5.2 Case 2: for TCP/IP Based Scheme

In the case of TCP/IP based scheme shown in Fig.4, all of cars download files from RSU. When cars request a file, they sent a request to RSU, RSU answers every request. And then

downloads the file from content-server and broadcasts it to cars. Every car obtains files only by the way of accessing content- server via RSU. The application case 1 and case 2 will be simulated in next section.

2.6 Simulation Parameters and Results

Both of application cases are simulated by the scenario that 400 cars are going into a metropolitan area and 100 files of proximity marketing will be distributed to every vehicle. The simulation is implemented by OMNeT++ 4.4.1 (network simulator), combining Veins 3.0 framework (vehicular network simulator) and SUMO 0.21.0 (road traffic simulator) [13]. A real-world road traffic in a metropolitan area (Sannomiya Kobe, Japan) produced by SUMO 0.21.0 is shown in Fig.5. We compared the in-network caching-based scheme with the legacy solution of TCP/IP based scheme in several aspects as below:

2.6.1 Impact of obstacles

In order to illustrate the impact of obstacles on file transmission, first, we offload the obstacle module of Veins to observe the results. We compared file capture rates (or received files by cars) of two schemes with equal simulation parameters shown in Table 1. 400 cars are entering this commercial area and plan to receive 100 files of proximity marketing contents. The results in Fig.6 show 100% and 94.2% of file capture rate for two schemes respectively. 400 cars can receive 100% files by proposed scheme. The legacy solution is not able to receive all of files because of serious dependency on RSU: some routes are far away from RSU coverage range so that the radio wave is attenuated and cannot reach to some cars. The proposed scheme could achieve 100% capture rate because caching nodes support the file delivery through V2V transmission even though radio wave from RSU cannot reach to some cars.

Secondly, we lead obstacle module of Veins into simulation program and repeat the experiment with the same parameters as given in Table I. The simulation results shown in Fig.7 present 99.3% file capture rate for LCE in-network caching scheme and 67.8% file capture rate for TCP/IP based scheme. Because buildings block radio propagation or attenuate the radio wave, file transmission becomes difficult [18][19]; file capture rate of legacy solution suffers much more severe influence than proposed scheme, and the file capture rate is decreased from 94.2% to 67.8%. Delightfully, the LCE in-network caching-based scheme is still able to keep a very high file capture rate of 99.3%.

Thus, the simulation results demonstrate the LCE caching scheme performs stronger robustness and stability against obstacles than legacy TCP/IP based scheme.

2.6.2 Evaluation on cache function

We will analyze a detailed file capture rate in this section. File capture rate is composed of two parts. One is contributed by cache nodes (V2V); another is contributed by RSU

infrastructure (V2I). The simulation results shown in Fig.8 present that file capture rate achieved between vehicle and vehicle transmission supplied by caching nodes (V2V) is dominant than between vehicle and infrastructure transmission supplied by RSU broadcast (V2I). Only a minimal fraction of 2.5% file is captured from RSU broadcast. Other 97.5% of files are captured by neighbor caching nodes. Thus, the cache function dominates the file delivery.

2.6.3 RSU broadcast frequency

Moreover, we counted the broadcast frequency of RSU in both schemes, to evaluate the dependency on RSU.

The numerical simulation results listed in Table II illustrate two scheme's dependency on RSU. During simulation time of 500 seconds, the broadcast frequency for proposed scheme is 200, which is much lower than 4798 of legacy solution. Besides, the received files provided by RSU broadcast also present significant difference of 999 and 27713, respectively. On the other hand, because RSU is connected with original content server, broadcast frequency of RSU is an indirect evaluation on internet traffics. Less broadcast represents less internet traffic.

The simulation results indicate that the proposed scheme enables less broadcasts from RSU infrastructure; thereby alleviates dependency on RSU infrastructure and decreases internet traffics.

2.7 Conclusion

We reviewed the related literatures of content distribution in ICN/CCN and vehicular network, and then proposed LCE (leave copy everywhere) in-network caching-based scheme applied on vehicular network for disseminating proximity marketing files in a metropolitan area. And LRU (least recently used) algorithm is applied in every cached node. This enlightenment is derived from next generation internet called ICN/CCN paradigm.

Proposed scheme based LCE in-network caching with LRU algorithm in all of cache is effective to deal with the typical issue of low data delivery ratio, which is caused by some typical reasons, e.g., obstacles in metropolitan areas, finite radio wave coverage range, limited APs deployment, and inefficient TCP/IP paradigm. Cache strategy LCE and algorithm LRU is employed according to the characteristic of vehicle communication in urban environments.

Simulation environments of OMNeT++ & Veins and SUMO provide powerful simulation tools to validate the proposed scheme. Comparing with the legacy solution of TCP/IP based scheme, LCE in-network caching scheme presents more robustness against obstacles and can achieve higher file capture rates. Besides, through analyzing file capture rate contributed by caching nodes (V2V) and RSU (V2I) respectively, we evaluated the cache function and conclude that file delivery achieved by V2V transmission is dominant. Furthermore, the

simulation results indicates that the proposed scheme enables less broadcasts frequency from RSU, thereby alleviates dependency on RSU infrastructure and reduces internet traffics.

LCE in-network caching-based scheme in vehicular networks opens a prospective direction for disseminating popular contents in metropolitan areas.

Chapter 3

Leveraging In-Network Caching in Vehicular Network for Content Distribution

3.1 Abstract

Information-Centric Networking advocates ubiquitous in-network caching to enhance content distribution. Non-safety application in vehicular communications is emerging beyond the initial safety application. However, content distribution based on TCP/IP Internet service in vehicular networks suffers from typical issue of low delivery ratio in urban environments, where high buildings block or attenuate the radio propagation as well as short radio coverage range. In order to solve this issue to deliver proximity marketing files, in this paper we propose in-network caching scheme in vehicular networks in accordance with traffic features, in which every vehicle is treated as either a subscriber to request a file or as a cache node to supply other nodes so as to accelerate file transmission effectively. Cache strategy of leave copy everywhere is uncoordinated and distributed, which fits the random and dynamic vehicular network. The performance evaluation is carried out by comparing the proposed scheme with the legacy solution of TCP/IP based scheme using simulation tools of OMNeT++ and Veins and SUMO, which is supplied with real-world urban map associated with random but reasonable traffic routes generated by our designed software for every vehicle. The simulation results validate the proposed scheme in four aspects: robustness resisting obstacle buildings, reliability and scalability in different traffic loads, low utilization ratios of RSUs and Internet resource, and efficiency of cache function.

3.2 Introduction

Information-Centric Network (ICN) has motived the development of future Internet architectures instead of the current Internet of host-to-host communication model [20–22]. The common goal of ICN is to achieve efficient and reliable content distribution by providing a general platform for communication services that are today only available in dedicated system such as peer-to-peer (P2P) overlays and proprietary content distribution networks [20, 21]. ICN lever- ages in-network caching to provide a better-performing and more robust

transport service. In-network caching has emerged as a distinct research field in the context of ICN [23].

Non-safety application in vehicular communications is emerging beyond the initial safety application such as driving safety and driving efficiency [24–27], underlying the trend that multimedia contents will represent more than 90% of the whole Internet traffics in a few years [28, 29]. Additionally, the delay tolerant data service of non-safety application in vehicular networks is recently considered to take advantage of sensor networks instead of relying on 4G-LTE Internet service. In-network caching embedded in vehicular networks becomes a prospective direction associating with the upsurge of new generation Internet because the characteristics of ICN match the requirement of vehicular networks, which is merely focusing on information itself in the most of cases rather than addressable vehicle entities like traditional IP networking paradigm.

In this paper, we address an application with respect to in- network caching technique leveraged in vehicular networks for proximity marketing file distribution in a metropolitan area, since cities as the centers of life and business are vitally important places to take advantage of the modern technologies to help people acquire information and to provide more comfortable experiences. We will review the recent developments, challenges, and related work and then propose in-network caching-based scheme in the next section.

3.3 Background

3.3.1 Existing Study

For vehicular communications, the automotive industry has standardized multiple radio and medium access technologies, for example, DSRC (Dedicated Short-Range Communications) and WAVE (Wireless Access in Vehicular Environments, IEEE 802.11p) for direct vehicle-to-vehicle communication (V2V) as well as RSU-to-vehicle communication (R2V) [25, 26, 30, 31]. Term “Short Range” in DSRC means that the communication takes place over hundreds of meters, a shorter distance than what cellular and WiMAX ser vices typically support [32]. This means when vehicles are travelling at normal speeds, they can exchange information each other like mobile communications.

Although the primary motivation for deploying DSRC is to enable collision prevention application, it is also able to be used for more general entertainment and commercial purposes beyond collision avoidance. Even though non- safety application offered by current DSRC technique is still restricted, we can foresee its extension in the future. Figure 2.1 shows an elemental scenario of the current TCP/IP based data delivery for non-safety application, which occurs between roadside units (RSUs) and vehicles through accessing Internet. RSU is a fundamental infrastructure as a bridge between Internet and vehicles. In this situation, RSU infrastructure is essential and unique equipment to deliver data to vehicles.

Currently safety application has been sufficiently investigated in many opened literatures. However, non-safety application is still underlying an initial stage. Some solutions can achieve good performance under the legacy TCP/IP paradigm. The literature in [25] indicates that coding techniques (coded storage) are effective for large files transmission over small files and could speed up the download of large files in vehicular networks. The work in [27] tackled content downloading in vehicular networks by optimizing APs (access points) deployment, V2V relay, and penetration rate. Although TCP/IP protocols have been proposed to run on top of vehicular networks for data exchange among vehicles [26, 30], a fundamental limitation is that the requirement of infrastructure support is essentially needed for global IP address allocation [26], which is somewhat infeasible to assume a sustainable availability on infrastructure support due to instability connectivity to RSU infrastructures such as radio attenuation caused by obstacle buildings and limited radio coverage range shown in Figure 2.1,aswellasrapidly expanded Internet traffics. Besides, the cost for RSU deployments is enormous in some countries, particularly in Japan, because of rare land resource and expensive construction cost. Thus, decreasing the utilization and dependency on RSUs have to be taken into account when designing a new scheme.

So far, few literatures of applying ICN to VANET (vehicular ad hoc networks) exist, with some examples being [24,26,31]. In [26], Wang et al. Proposed instructive idea in data naming, routing, data structure, and so on. In [24], the proposed framework called ICNoW (Information-

Centric Networking on Wheels) focuses on the content and its scope in space, time, and user interest. In [31], the design called content-centric vehicular networking focuses on naming data, retrieval process, and preliminary evaluations and concludes that ICN outperforms the legacy solution of TCP/IP when consumers increase.

Our work in this paper addresses an in-network caching-based scheme shown in Figure 2.2, which aims at solving the issue of low data delivery caused by obstacle buildings and short radio coverage range in a metropolitan area for proximity marketing file distributions. The proposed scheme makes an effort to achieve high data delivery ratios and to reduce the access frequency to RSUs and the Internet traffic by adding vehicle-to-vehicle communication model since every vehicle is equipped with an on-board cache. In-network caching based V2V communications enable effectively overcoming the impact from obstacle buildings and limited radio coverage range compared to R2V communications so as to improve data delivery ratios.

We employ leave copy everywhere (LCE) cache strategy and broadcast on-path routing to vehicular networks, as well as proposing least recently used (LRU) replacement algorithm running in all of caches according to the characteristics of vehicular dynamic movements and frequent information exchange in commercial environments. Every vehicle plays a role of not only a subscriber to require files, but also an in-network cache for responding to other vehicles requirements.

We evaluate in-network caching-based scheme with legacy solution of TCP/IP based scheme in four aspects.

3.3.2 Robustness Evaluation

First, how much impact on data transmission caused by obstacle buildings is evaluated for the two schemes by comparing their file delivery ratio using a middle traffic load scenario. Proposed in-network caching-based scheme performs stronger robustness and stability in both of situations: whether the obstacles exist or not. In contrast, the data delivery ratio of legacy TCP/IP based scheme is seriously impacted, decreasing by obstacles. Proposed scheme performs more robust for resisting obstacle buildings.

3.3.3 Reliability and Scalability Evaluation

An effective scheme should keep up a steady performance in various traffic situations: low, middle, or high traffic load. Simulation results. of proposed scheme in different traffic loads present reliable, stable, and high data delivery ratios whether there are obstacle buildings or not; however, TCP/IP based scheme is obviously inferior to proposed one especially when obstacle buildings exist. Moreover, the good performance under the high traffic load demonstrates that the proposed scheme is appropriate for scalability applications.

3.3.4 Low Utilization of RSUs and Internet Resource

RSU is a bridge between vehicles and Internet. On one hand, the broadcast frequency of RSUs represents how much service has been provided to the vehicles. On the other hand, it is an indirect metric to estimate Internet traffic. In our experiment setup, the more broadcast number of RSUs means the more utilization of RSUs, so the more dependence on RSUs the more consumption of Internet traffics. The simulation results indicate the proposed scheme performs much less broadcast frequency than TCP/IP based scheme. The proposed in-network caching undertakes major of file delivery relying on vehicle-to-vehicle communication instead of RSU-to-vehicle communication; however, in the legacy scheme, the file delivery only depends on RSU-to-vehicle communication, so that the legacy scheme has more broadcast sent from RSU compared to the proposed scheme.

3.3.5 Cache Efficiency Evaluation

In-network cache is a core technique in the proposed scheme. The data deliver y ratio is significantly improved by the cache function that undertakes vehicle-to-vehicle communications instead of a large portion of RSU-to-vehicle communications. In order to demonstrate this, we give a quantitative analysis on data delivery ratios of V2V communication and R2V communications, respectively, in different traffic loads to evaluate the cache efficiency.

The remainder of this paper is organized as follows. In Section 3, we propose in-network caching-based scheme through analyzing the key issues and challenges, while legacy TCP/IP based scheme is also presented for comparison with the proposal. Additionally, two application cases corresponding to the proposed and compared schemes, respectively, are described. In Section 4, the simulation-based validations with discussions are carried out in various traffic scenarios.

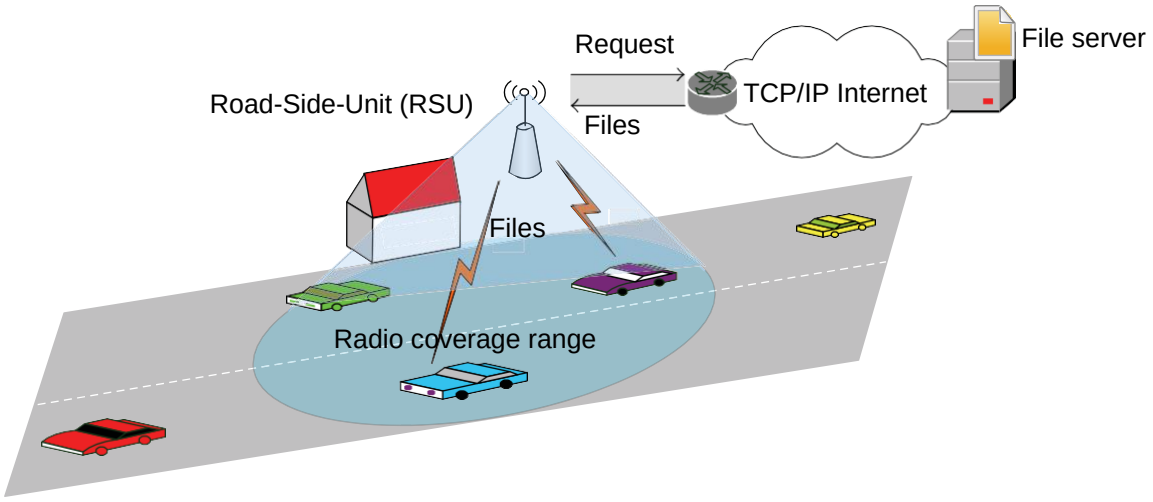

Fig. 3.1. TCP/IP based file delivery scenario

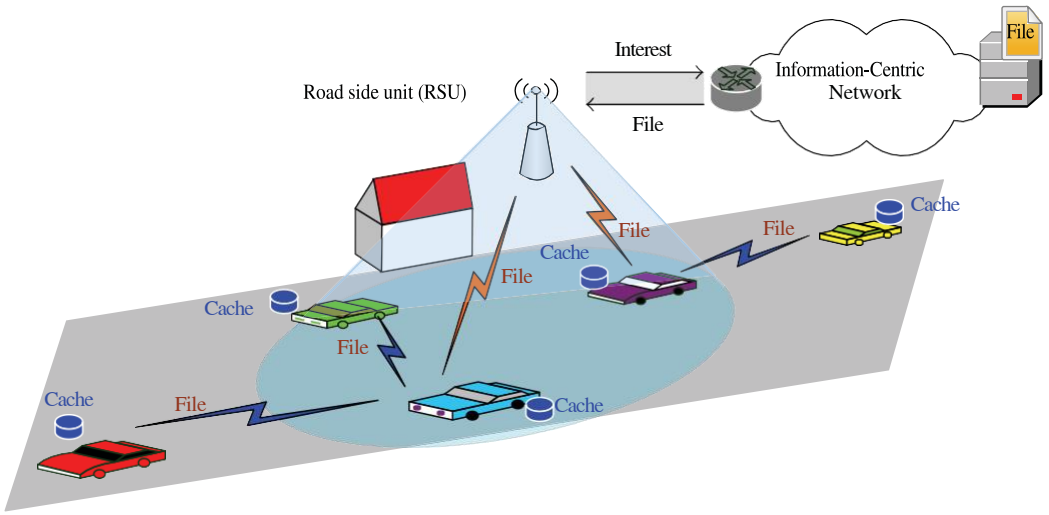

Fig. 3.2. In-network caching-based file delivery scenario

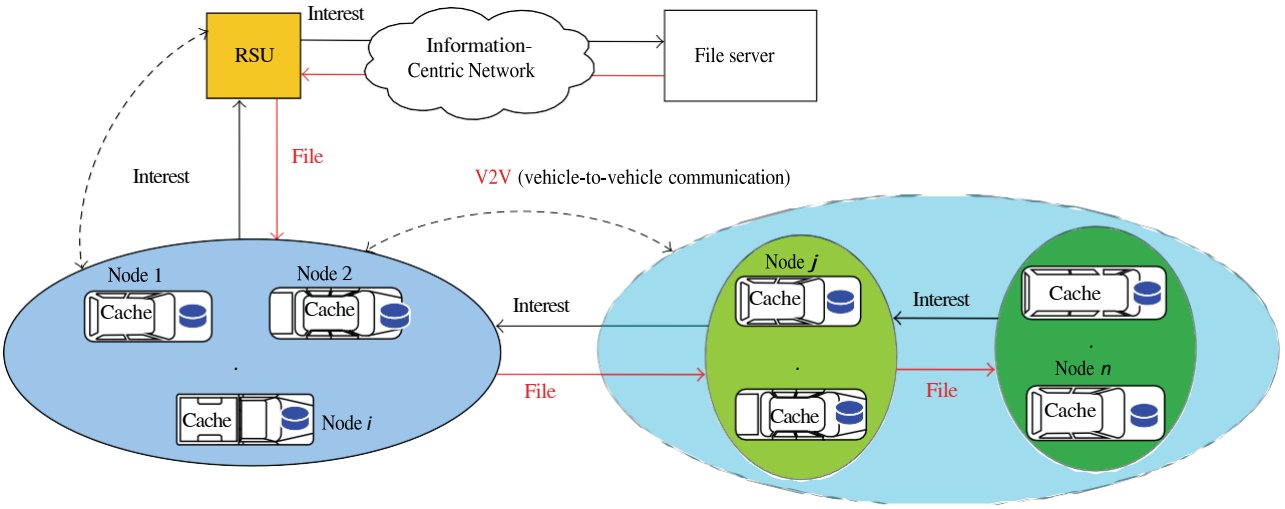

Fig. 3.3. The flowchart of file transmission for proposed in-network caching based scheme

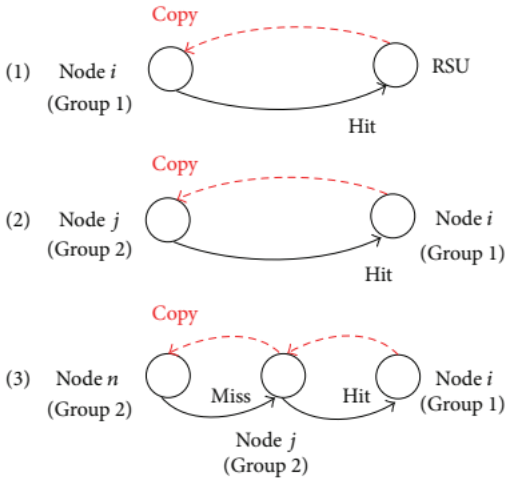

Fig. 3.4. Cache strategy of proposed scheme

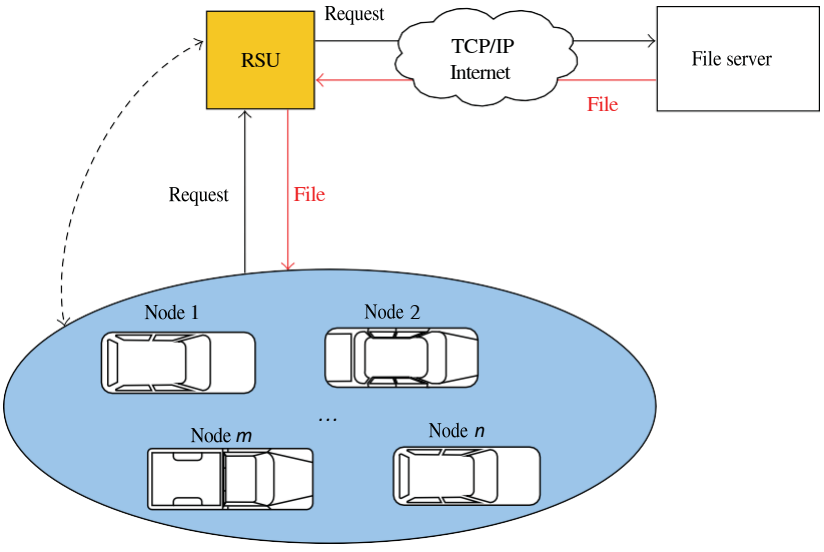

Fig. 3.5. The flowchart of file transmission for TCP/IP based scheme

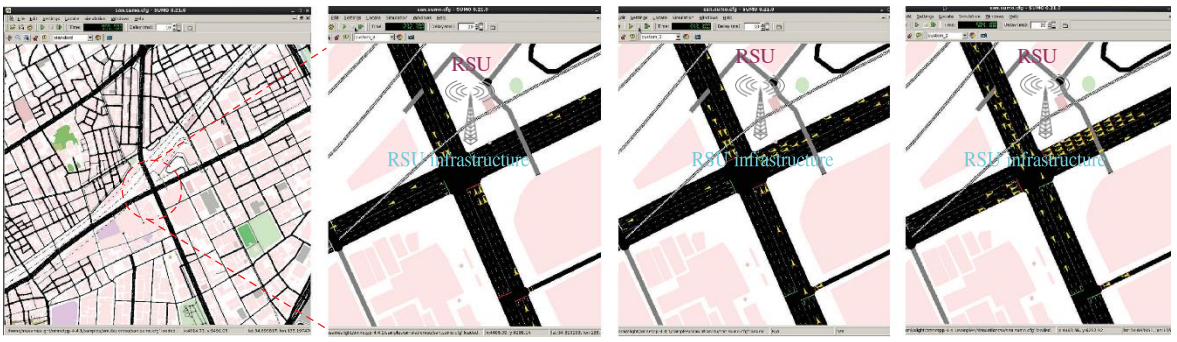

Fig. 3.6. Simulation map and scenarios

TABLE 3.1 Simulation parameter

Parameter	Value
Location	Latitude: 34.*6882~6978*; longitude: 135.*1864~2017*
Vehicle number	300 and 600 and 900
RSU number	1
File size	1.5 KB
File number	100
Simulation time	600 s
Period of entering into roads	0~200 s
Beacon interval and broadcast interval	1 s
Broadcast interval	0.1 s
Max. transmission power	20 mW
MAC bit rate	18 Mbit/s
Transmission range	300 meters

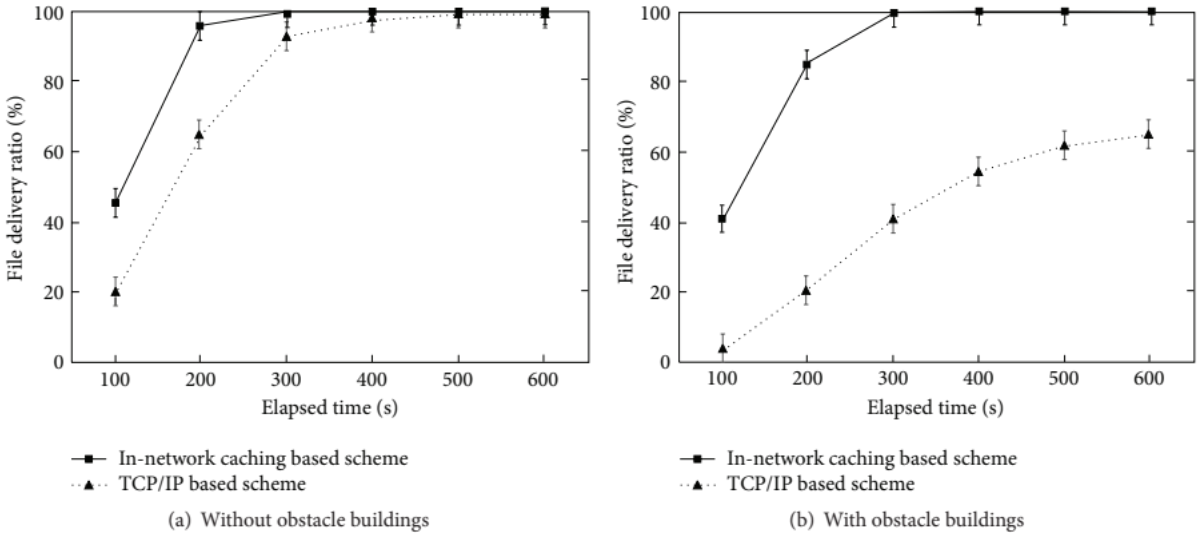

Fig. 3.7. File delivery ratios in a middle traffic load of 600 vehicles.

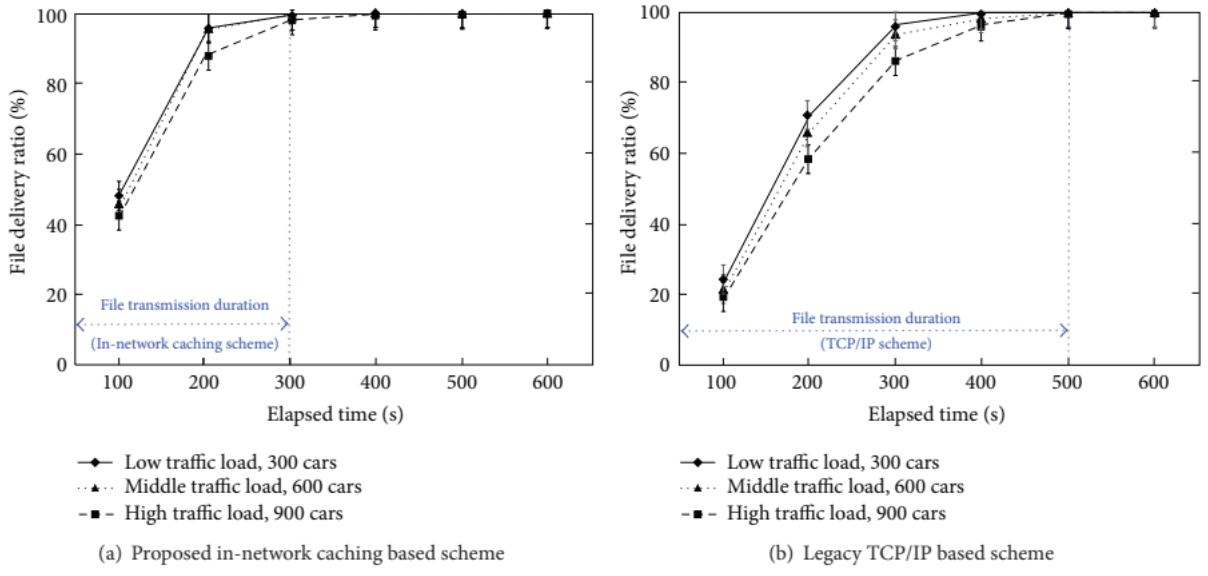

Fig. 3.8. File delivery ratios in different loads without obstacles.

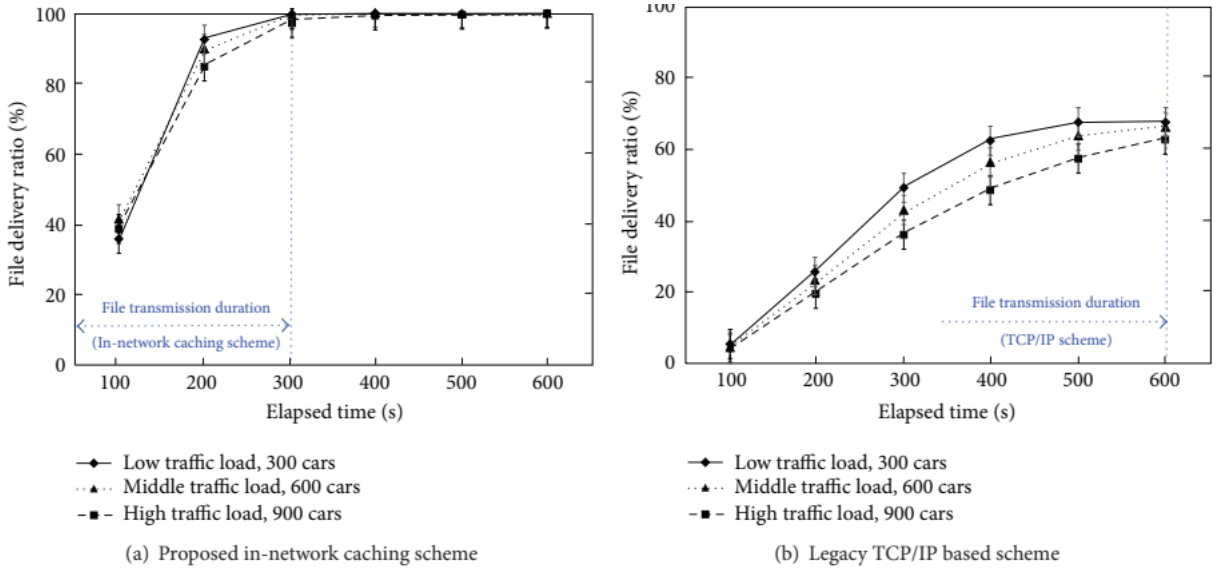

Fig. 3.9. File delivery ratios in different loads with obstacles.

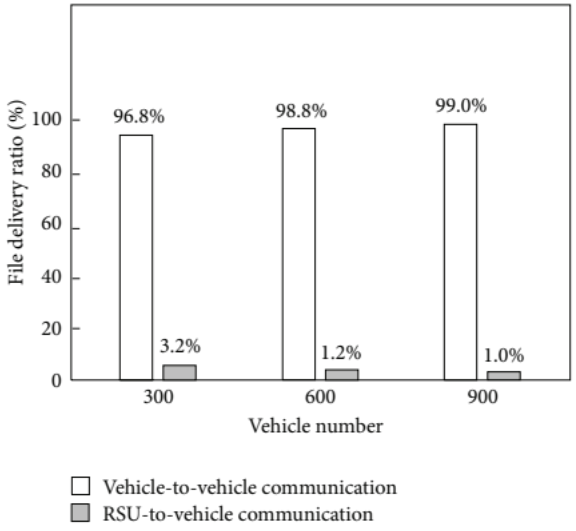

Fig. 3.10. File delivery ratios achieved by V2V and R2V communications.

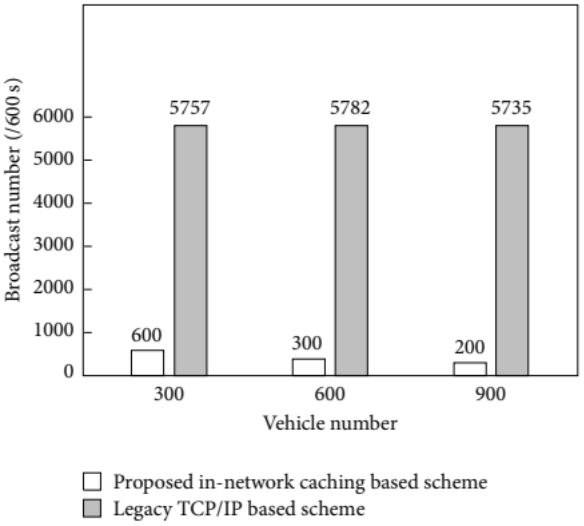

Fig. 3.11. Broadcast number in low, middle, and high traffic load.

3.4 Proposed In-Network Caching Based Scheme and Legacy Solution of TCP/IP

3.4.1 Our Proposal: In-Network Caching Based Scheme

Data transmission in vehicular networks suffers from a typical issue, low data delivery ratio in urban environments, where high buildings block or attenuate the radio propagation emitted from RSU infrastructures [31, 38]. On the other hand, other technical issues, for example, absolute necessity of connectivity with RSU for global IP address allocations, short radio wave coverage range, and limited Aps (access points) deployment, cause serious dependency on RSU infrastructures. Although more RSUs could be deployed to increase coverage range of radio wave, it is deviated from the trend of reducing the cost of expensive infrastructure deployments and eliminating network traffics.

Increasing RSU deployment that is treated as an alternating solution in some literatures could well improve data transmission [27, 39], even though multi-RSU synchronization and capital costs are still difficult to be tackled [40, 41]. The multi-RSU deployment can enhance data transmission, but the improvement is not infinite for the sake of inherent nature of DSRC equipment and geographical environments.

Above issues are difficult to be tackled by legacy solution so that impels us to explore new solutions toward ICN paradigm. Considering overcoming the capital costs of ubiquitous RSU and developing more efficient data transmission scheme, another solution that facilitates data transmission between vehicles is addressed in this paper. The solution scheme should allow mobile nodes to dynamically create.

storage points for contents that could be distributed more quickly and more robustly. In-network caching is a prospective technique to achieve this.

Although there are sufficient cache strategies proposed for ICN in previous works, for example, LCD (leave copy down), MCD (move copy down), Prob (copy with probability), and ProbCache (a weighted probability cache) [42– 45], due to the vehicular characteristics of mobility, short- lived and intermittent connectivity, the caching strategy has to be uncoordinated and distributed, which fits the random, dynamic, and unstable features in V2V communication. Thereby in-network caching scheme called leave copy everywhere (LCE) for every vehicle is borrowed for V2V communication in our work. LCE can extend radio coverage range and decrease relay time.

Besides, least recently used (LRU) replacement algorithm is proposed to run in all of caches. In a commercial region, proximity marketing files are concerned by people. LRU algorithm in caches is reasonable according to the link popularity.

In the proposed vehicular network shown in Figure 3.2, every vehicle plays two roles as not only a subscriber for requiring files, but also an in-network cache for responding to other vehicles interests and forwarding files to them. The caches store high popular proximity marketing files and undertake data delivery instead of frequent connectivity with RSU infrastructure without considering the impact of obstacle buildings so as to accelerate the file delivery effectively and mitigate the dependency on RSU.

The flowchart of application cases is shown in Figure 3.3. The target is to make all nodes capture the same file that is initially placed in a server. In the first step, RSU downloads the file from the server to respond to the Interest from the vehicular network. Secondly, the file is broadcasted by RSU to the vehicular network. A fraction of vehicles received the file by RSU-to-vehicle communication and cache this file; these cars belong to Group 1. Other vehicles that do not receive the file from RSU belong to Group 2. The file is spread to Group 2 through vehicle-to-vehicle communication.

The cache policy of Group 1 is shown in (1): after node i downloads the file from RSU, it caches this file. The cache policy of Group 2 is shown in (2) and (3). The nodes in Group2 download file by two ways. One way is shown in (2): after node j gets the file from node i of Group 1, it caches this file. The other way is shown in (3): node n requests file via relay node j of Group 2tonode$i$ of Group1. On the back way, the file is cached in every node. Above operations are applied in every node.

Furthermore, in order to increase data transmission happening between vehicle nodes (V2V communication) and reduce the utilizations of RSUs, we set up RSU broadcast frequency by responding to one per 10 interests.

3.4.2 Legacy Solution: TCP/IP Based Scheme

In the scenario of legacy scheme shown in Figure 3.1, all of vehicles capture files through RSU-to-vehicle communications. Although the file delivery could sometimes happen through V2V relay, indeed the last relay node still needs a connection with infrastructures. In another word, all cars must capture data from RSU directly or indirectly. In accordance with this situation, we simplify the data delivery routes: assume all of cars capture data from RSU infrastructures. The vehicular network is seriously relying on RSU support.

Based on a condition of fair RSU resource, one RSU, same as proposed scheme, is deployed in legacy scheme. Thus, an application case of TCP/IP based scheme is shown in Figure 3.5 for comparison with proposed scheme. When nodes request a file, they send a request to RSU, and RSU answers every request. And then RSU downloads the file from the server and broadcasts it to the nodes. Every car acquires the file only through the way of accessing the server via RSU. RSU-to- vehicle communications are the sole communication way in TCP/IP

based scheme. The two application cases of the proposed and legacy schemes will be simulated in various scenarios in the next section.

3.5 Performance Evaluation

In this section, we present various traffic scenarios for the evaluation of the proposed scheme with experiment environments, simulation results, and corresponding discussions. Vehicles are going into a metropolitan area called Sannomiya of Kobe in Japan shown in Figure 3.6 (a), which is a real-world urban map downloaded from OpenStreetMap, and 100 files of proximity marketing will be distributed to these vehicles in this area. The simulation is implemented by OMNeT++ 4.4.1 (network simulator), combining with Veins 3.0 framework (vehicular network simulator) and SUMO 0.21.0 (road traffic simulator). Besides, we generated the traffic routes for every vehicle by designing proprietary software, so reasonable traffic routes are able to be provided. This traffic system makes the simulation results more reliable for validation. If zooming in the central location, the RSU setup location and the vehicle movements in low, middle, and high traffic loads can be observed in Figures 3.6 (b), 6(c), and 6(d), respectively. The simulation parameters are listed in Table 3.1. The performance evaluation is carried out in four aspects as below.

3.5.1 Robust Evaluation

In the How much impact on data transmission caused by obstacles is evaluated for the two schemes by comparing their file delivery ratios using a middle traffic load scenario of 600 vehicles. First, we offload the obstacle module from Veins to observe the results. We compared the file delivery ratios of two schemes with the equal simulation parameters. The results without obstacles are shown in Figure 3.7 (a). Both of schemes can achieve approximately 100% of file deliver y ratios. This means, in the environment without obstacle buildings, the in-network caching scheme does not perform obvious advantage in data delivery ratio, certainly it performs a little well in speed.

Second, we lead obstacle module into simulation programs and repeat the experiment with the same parameters. Proposed in-network caching scheme still presents approximately 100% of file delivery ratio; however, the percentage is only 64.8% for TCP/IP based scheme, shown in Figure 3.7 (b).

Since obstacle buildings block radio propagation or attenuate radio wave as well as the limited radio coverage range, the file delivery ratio of legacy scheme suffers from serious lessening. Fortunately, the proposed in-network caching-based scheme performs stronger robustness in both of situations: whether the obstacles exist or not.

3.5.2 Reliability and Scalability Evaluation

An effective scheme should keep up a steady performance in various traffic situations, so we provide 300, 600, and 900 vehicles corresponding to the low, middle, and high traffic loads.

First, the simulation results without obstacle modules for proposed scheme are shown in Figure 3.8 (a). The file transmission duration shown in each figure reflects the speed of accomplishing file delivery. There is no obvious difference in file delivery ratio and speed between various traffic loads for proposed scheme. The file delivery ratio is 100% and the file transmission duration is 300 s. For the TCP/IP based scheme, the data delivery ratios shown in Figure 3.8 (b) also reach approximately 100% even if TCP/IP based scheme takes longer transmission time of 500 s. In the point of processing speed, proposed scheme performs better than legacy scheme.

Second, the simulation results with obstacle modules are shown in Figures 3.9 (a) and 3.9 (b), respectively. Compared with Figures 3.8 (a) and 3.8 (b), in different traffic loads the proposed scheme always presents reliable, stable, and high data delivery ratios whether there are obstacle buildings or not. However, for the TCP/IP based scheme, file delivery ratio is obviously decreased and file transmission duration is increased, which is exceeding 600 s.

Moreover, the good performance in a high traffic load demonstrates that the proposed scheme is appropriate for the scalability applications.

3.5.3 Cache Efficiency Evaluation

In-network caching is the core technique in the proposed scheme. The data delivery ratio is significantly improved due to the cache function that undertakes vehicle-to-vehicle communications instead of a large portion of RSU-to-vehicle communications. In order to demonstrate this, we give a quantitative analysis on data deliver y ratios of V2V communication and R2V communications, respectively, in the different traffic loads to evaluate the cache efficiency.

The statistics data shown in Figure 3.10 demonstrates that V2V communications are the over whelming majority in the data delivery process, which means the in-network cache participates in the major file delivery instead of R2V communications.

3.5.4 Low Utilization of RSUs and Internet Resource

RSU is a bridge between vehicles and Internet. On one hand, the broadcast number of RSUs represents how much service has been provided to vehicles. On the other hand, it is an available metric to estimate Internet traffic. In the simulation setup, the more broadcast number of RSUs means the more data requests for RSUs and so the more dependence on RSU and the more consumption of Internet traffics.

The broadcast number of RSUs is aggregated for both schemes with obstacle modules under the low, middle, and high traffic loads shown in Figure 3.11. The data presents considerable difference from several hundreds to 6 thousand or so. In the legacy scheme, vehicles receive files only from RSU; contrastively in the proposed scheme vehicles receive most of files from vehicles rather than RSU, which is depicted in Figure 3.10. Thereby the broadcast from RSU in legacy scheme is much more than proposed scheme. The proposed scheme shows much lower utilization of RSU and Internet resource.

3.6 Conclusion

We reviewed the related literatures of content distribution in vehicular networks and Information-Centric Networking and then proposed in-network caching-based scheme in vehicular networks associated with leave copy everywhere strategy for disseminating proximity marketing files in urban environments. Additionally, least recently used algorithm is suggested for every cached node. This enlightenment is derived from next generation Internet of ICN paradigm.

The proposed in-network caching scheme is effective to deal with the typical issue of low data delivery ratio in metropolitan areas, which is caused by obstacle buildings, short radio coverage range of RSU, limited RSU deployment, and crowded TCP/IP traffics. In-network caching is a core technique in the proposed scheme. The data delivery is significantly improved by cache function that undertakes vehicle-to-vehicle communications instead of a large portion of RSU-to-vehicle communications.

The performance evaluation is carried out by comparing the proposed in-network caching-based scheme with the legacy solution of TCP/IP based scheme using power simulation tools of OMNeT++ and Veins and SUMO, which is supplied with a real-world urban map associated with random but reasonable traffic routes generated by our designed software for every vehicle. The simulation results validate the proposed scheme in four aspects: robustness for resisting obstacle buildings, reliability and scalability in different traffic loads, low utilization of RSUs and Internet resource, and excellent efficiency of cache function.

In-network caching-based scheme in vehicular networks opens a prospective direction for content distribution in urban environments.

Chapter 4

CCN-Based Vehicle-to-Vehicle Communication in DSRC for Content Distribution in Urban Environments

4.1 Abstract

Dedicated Short Range Communication (DSRC) is currently standardized as a leading technology for the implementation of Vehicular Networks. Non-safety application in DSRC is emerging beyond the initial safety application. However, it suffers from a typical issue of low data delivery ratio in urban environments, where static and moving obstacles block or attenuate the radio propagation, as well as other technical issues such as temporal-spatial restriction, capital cost for infrastructure deployments and limited radio coverage range. On the other hand, Content- Centric Networking (CCN) advocates ubiquitous in-network caching to enhance content distribution. The major characteristics of CCN are compatible with the requirements of vehicular networks so that CCN could be available by vehicular networks. In this paper, we propose a CCN-based vehicle-to-vehicle (V2V) communication scheme on the top of DSRC standard for content dissemination, while demonstrate its feasibility by analyzing the frame format of Beacon and WAVE service advertisement (WSA) messages of DSRC specifications. The simulation-based validations derived from our software platform with OMNeT++, Veins and SUMO in realistic traffic environments are supplied to evaluate the proposed scheme. We expect our research could provide references for future more substantial revision of DSRC standardization for CCN-based V2V communication.

4.2 Introduction

Dedicated Short Range Communication (DSRC) is a standard that initially aims to bring vehicular networks to North America, meanwhile also has been considering world widely in other regions and countries, i.e., Europe and Japan [46], [47]. DSRC is emerging as a leading technology for the implementation of Vehicular Ad-hoc Networks (VANETs). The second generation of DSRC technology in the 5.9 GHz band has the potential to support different types of application, e.g., active safety, public service, improved driving, business and

entertainment [48]. Internet- related content downloading as one of non-safety application has been more concerned in delay-tolerant networks in the context of sufficiently exploiting vehicular resource for more convenience and comfortable life [49]–[51]. However, the Internet-based content distribution between vehicle and vehicle for non-safety application has not been sufficiently discussed in DSRC. And the key for developing localized vehicular non-safety application is information content it- self, rather than addressable vehicle entity like traditional IP networking paradigm [52].

On the other hand, Information-Centric Networking (ICN) has motived the development of future Internet architectures based on named data objects (NDOs), instead of the current internet of host-to-host communication model [53]– [56]. The characteristics of Content-Centric Networking (CCN) as one of ICN oriented projects match this requirement of vehicular networks, which is only focused on con- tent itself not content source location. Exploiting CCN in vehicular communications could become a prospective direction.

In this study, we propose a CCN-based V2V communication scheme on the top of DSRC standard for content dissemination, while demonstrate its feasibility by analyzing the frame format of beacon and WSA (WAVE service advertisement) messages. According to the characteristic of vehicular networks, hierarchical structure of naming, on- path routing, Leave Copy Everywhere of cache strategy and least frequently used algorithm are assigned for vehicular CCN paradigm. Effective validations based on our software platform with simulations tools in realistic traffic environments are implemented. We expect CCN-based V2V communication for content distribution in urban environments could provide reference for future more substantial revision on DSRC standard.

4.3 Background, related works and Our Contributions

4.3.1 Background

The major DSRC standard includes the IEEE 802.11p amendment for Wireless Access in Vehicular Environments (WAVE), the IEEE 1609.2, 1609.3, and 1609.4 standards for security, network service, and multi-channel operation [57]– [59]. Vehicle-to-vehicle (V2V) based application supported by DSRC standard is restricted to basic safety message exchange for safety purpose [60], [61]. In order to modify DSRC standard for non-safety application, a brief description of DSRC protocol stack well documented and illustrated in some literatures [57]–[59] is briefly illustrated in Fig. 4.1 (a). TCP/UDP/IPv6 is used by only service channels and WAVE Short Message Protocol (WSMP) is used in both control and service channels.

WSMP is mostly used for safety applications and service, TCP/UDP/IPv6 stack is planned only for Internet-data service. One common control channel (CCH 178) on a fixed frequency is reserved for transporting control and safety messages; six service channels (SCH) are mainly used for exchanging non-safety data [59], as well as some safety- related information. Due to the channel-switch mechanism, content distribution becomes possible despite the safety application is always given priority over non-safety application.

In DSRC, data service could occur from a content server (or a remote host) to moving vehicles using access point such as road-side unit (RSU), which rely on a stable and reliable wireless link between vehicles with RSUs [62], which communication scenario is shown in Fig. 4.1 (b). The vehicles could be offered content files through WSA service happened in RSU-to-vehicle (R2V) communication.

For content distribution, the current working mechanism of DSRC meets some issues. IP-based data service in DSRC is restricted with its temporal-spatial property. On one hand, in a harsh vehicular environment, the link for every vehicle could not be guaranteed: vehicles stay within the wireless range of a road-side unit (RSU) only for a short duration within which it needs to complete a given service transaction [63]. Besides, obstructions of high buildings in urban environments block or attenuate radio propagation so that packet delivery ratio is seriously impacted [61], [63]– [65]. On the other hand, in an early stage of RSU deployment for DSRC, radio coverage of RSUs is technological limited as well as considerable capital expenditure and maintenance overhead [48], [66]. Moreover, in the situation that currently internet band width almost reaches limitation [53], it is difficult to complete downloading a file within the radio coverage scope [48], [63].

The ICN approach fundamentally decouples information content from its source address, which is fit the requirement of vehicular networks and mitigates the temporal-spatial

limitation that is shortness in existing DSRC service. Thereby we consider CCN should be added into DSRC for content distribution in V2V communication that currently only enables WAVE short message (WSM) for safety application in DSRC standard.

So far, a few opened literatures evaluate ICN applied to VANET with a modification of current communication standard DSRC and with effective validations in a real traffic environment with massive cars, some examples being [61], [67]-[69] indicate a direction forward CCN. In [62], slight modifications to the DSRC standard is proposed to improve RSU-awareness for WSA-based non-safety application.

In [68], L. Wang et al. proposed named data and de- signed the data structure in vehicular communication. Literature [67] proposes content-centric vehicular networking paradigm completely instead of TCP/UDP/IP in the network layer of DSRC.

In [70], parked cars are used for content downloading instead of relying on RSUs only, which extends the RSU ser- vice coverage. The work in [70] tackled content downloading in vehicular networks by optimizing APs (access points) deployment to increase data penetration rate.

In [16] a CCN paradigm is applied in a vehicular net- work performs more efficient and robust for content distribution in obstruction environments by simulation-based validation.

Increasing RSU deployment served as an alternating solution in some literatures can well improve data trans- action [60], [71], even though multi-RSU synchronization and capital costs are still difficult to be tackled.

F. Baietal. in [66] took a top-down framework called Information-Centric Network on Wheel to develop generic network architecture for supporting spatially-temporally localized and data-intensive vehicular application. Authors suggest the developed protocols for information management should allow for in-network data aggregation, storage, replication, and both push-based dissemination (TCP/IP) and on-demand pull-based querying (CCN). These instructive opinions enlighten the new scheme design in our work.

In [72], authors proposed a novel vehicular information network architecture to support location-based forwarding, content aggregation and distributed mobility management.

In [73], a cluster-based organization of vehicles is de- signed based on named data networking. Reference vehicles named barycenter plays router role to improve the chance of finding contents.

In view of afore mentioned, a solution scheme named CCN-based V2V communication for content distribution in metropolitan areas is proposed to run on top of DSRC shown in Fig.

4.2. This design derives from the enlightenment of in- network caching technique of CCN. In-network caching is employed to facilitate data propagation through V2V communication. The main contribution of this paper is summarized as follows:

1. Propose a coexistence of TCP/UDP/IPv6 and CCN paradigm in DSRC standard stack for more efficient content dissemination. IPv6 is used for content offering to vehicular networks by server-RSU-vehicle communications; CCN paradigm is used for content propagation in vehicular networks by vehicle-to-vehicle communication.

2. Analyze the feasibility with respect to availableness of CCN for vehicular networks and possibility of adding CCN protocol (CCNP) on DSRC standard. Through piggybacking content name on a beacon frame, an Interest of CCN could be achieved. A modified WSA (WAVE service advertisement) message is recommended for announcing CCN service and channel availability when operating CCN framework on DSRC.

3. Propose hierarchical structure like a web URL for naming, broadcast of on-path routing, and Leave Copy Everywhere for cache strategy in vehicular CCN.

4. Simulation-based validation is carried out by our soft- ware platform with simulation tools of OMNeT++ 4.4.1, Veins 3.0 framework and SUMO 0.21.0. We made program for CCN protocol used in simulation. The traffic routes for every vehicle are generated by self-developed system. The real-world traffic system with massive cars enables the simulation results more reliable for evaluation.

4.4 Proposed Scheme

Based on afore mentioned, we propose a coexistence of IPv6 and CCN paradigm in DSRC protocol stack shown in Fig. 4.2 (a) for more efficient content dissemination. Considering avoid radical changes in DSRC standard, the TCP/UDP/IP protocols for IP packets delivery is remained, which is working only in RSU-to-vehicle communication for content downloading from a server to vehicles via a RSU. A CCN protocol is designed into transmission and network layers to participate in the V2V communication for content propagation in the vehicular network. In MAC layer, specific service channels for IP packets and CCN packets are designated respectively. In WSMP, the piggybacked beacon is proposed as an Interest message for requesting a content file. A modified WSA message is exploited to announce content name and its service channel on which the CCN packets could be transmitted.

Corresponding to Fig. 4.2 (a), CCN-based data delivery scenario is shown in Fig. 4.2 (b). For a fraction of vehicles, content offering is relied on RSU-to-vehicle (R2V) communication, which is supported by TCP/UDP/IP protocol in network layer. Content distribution among vehicles is relied on vehicle-to-vehicle (V2V) communication, which is supported by CCN framework. In-network caching can facilitate data propagation through V2V communication.

4.5 Feasibility Analysis for Proposed Scheme

4.5.1 CCN Could Be Available by Vehicular Networks

The various ICN initiatives aim to address different Inter- net's problems and limitations by designing new Internet architectures. CCN is characterized by the basic exchange of content request messages (called "Interests") and content re- turn messages (called "Content Objects") [74]. CCN could utilize in-network caching technique that holds copies of de- sired information to assist information spread between vehicles in urban environments.

The essence of CCN lies in decoupling contents from host not at the application lever, but at the network level, which is well introduced in some literatures [53], [54]. In CCN, the location of a content file is independent of its name. Publish/subscribe is the main communication model: a content source announces (or publishes) a content file, while a user requests (or subscribes) to the content file. With publish/subscribe paradigm by in-network caching, the con- tent generation and consumption are decoupled in time and space, so contents are delivered efficiently and scalable.

4.5.2 Naming

CCN introduce a hierarchical structure to name a con- tent file like a web URL (e.g. /www.kobe.com/morii-lab/shiraishi v1), where / is the delimiter between components of a name. This naming mechanism is compatible with current URL-based applications, which also may imply a lower deployment hurdle when merge CCN protocol and TCP/UDP/IP into a vehicular network. Its hierarchical nature can help mitigate the routing scalability issue since routing entries for contents might be aggregated [54].

4.5.3 Routing

CCN just replace network prefixes (in IP routing) with con- tent identifier (like IP address), so the modification of IP routing protocols and systems may not be difficult [53]. CCN suggests inheriting IP routing, thus has compatibility to a certain degree. Therefore, CCN might be deployed incrementally with current IP network [8]. In vehicular networks, IP paradigm is still remained for data offering by RSU-to-vehicle communication, thus CCN might be the best candidate in our work due to its compatibility to IP routing.

4.5.4 Caching

CCN natively supports on-path caching [75], [76], since each content router first consults its content storage when- ever it receives an Interest message and caches all content objects [53]. The integration of router and storage makes routing simplified, which is fit the dynamic and

complicated vehicular network. How to achieve Advertisement and Interest messages of CCN in DSRC specification will be illustrated in the upcoming subsection.

4.5.5 Proposed CNN Vehicular Networks

Because the topology of vehicular network is dynamic, it is difficult to maintain routing tables; hence, the routing advertisement (for contents) is mainly performed by broadcast model. Figure 4.3 shows a procedure of a file distribution. The WSA service offers a file to vehicle-A from RSU via content server, and caches it. This file will be distributed using CCN paradigm by vehicle-to-vehicle communication. The vehicle A advertises the file name and service channel by WSA message. The vehicle B sends an Interest for requesting this file. The requested content name is piggybacked in a beacon as Interest message. The prefix matching rule is working for a decision in vehicle-A. If a matched file is found, vehicle-A immediately sends this file to vehicle-B, otherwise vehicle- A broadcast Interest beacon to other vehicles.

4.6 Possibility of DSRC Standard Used for CCN

To leverage CCN in vehicular networks will result in sophisticated amendment on DSRC standard. Quantity of specifications and frame format might be involved in. In this paper, only limited efforts defining Advertisement and Interest messages, are done.

4.6.1 Modify WSA Message Acting as Advertisement Message to Announce Content Name and Service Channel

Figure 4.1 (a) illustrates the protocol stack for DSRC [57], [58]. At the PHY and MAC layers, DSRC utilizes IEEE 802.11p for wireless access for vehicular environments, a modified version of the familiar IEEE 802.11p (Wi-Fi) standard. In the middle of the stack, IEEE 1609 framework specifies the networking services (1609.3) and multi-channel operation (1609.4). DSRC supports Internet protocols for the network and transport layers, i.e., Internet Protocol version 6 (IPv6), User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). In Fig. 4.2 (a), added CCN protocol is used to content service for V2V communication.

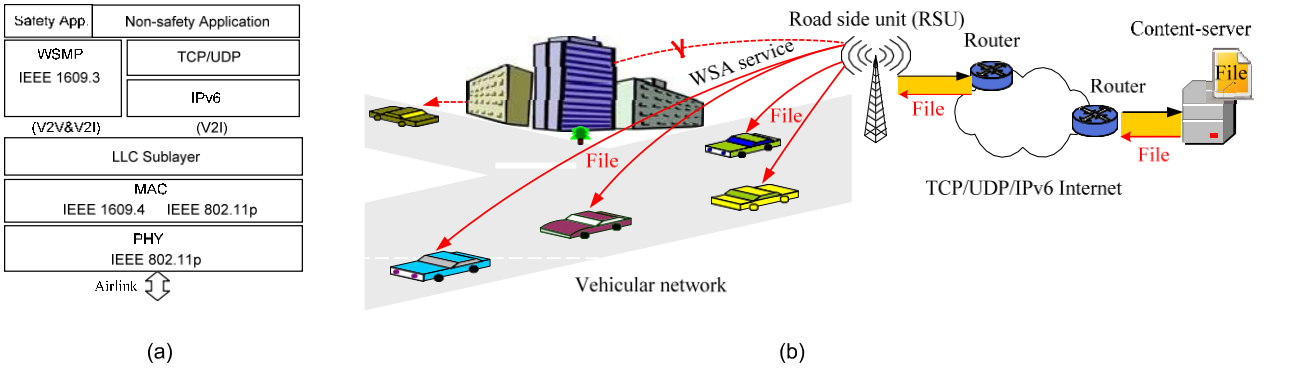

Fig. 4.1. DSRC-based scheme with (a) DSRC protocol stack and (b) content distribution scenario.

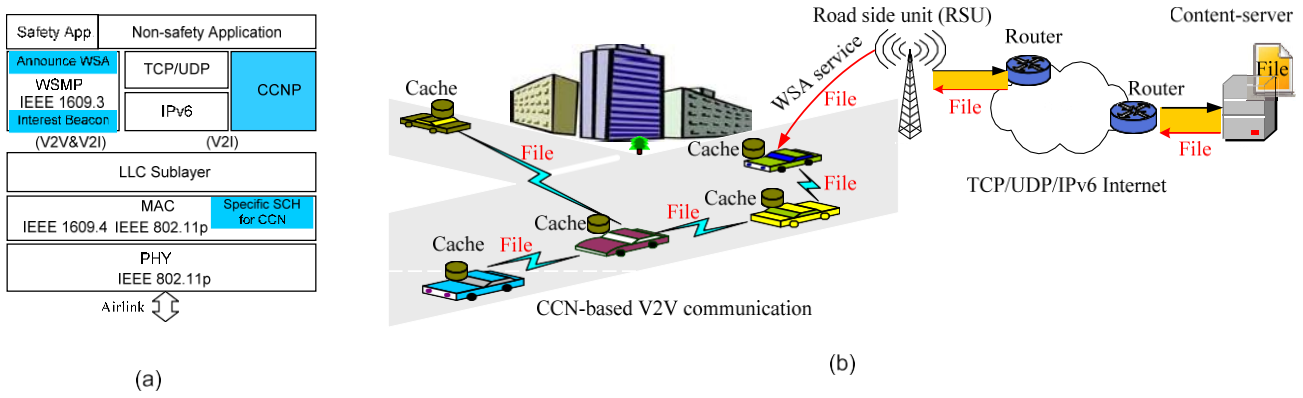

Fig. 4.2. Proposed CCN-based scheme with (a) CCN-DSRC protocol stack and (b) content distribution scenario.

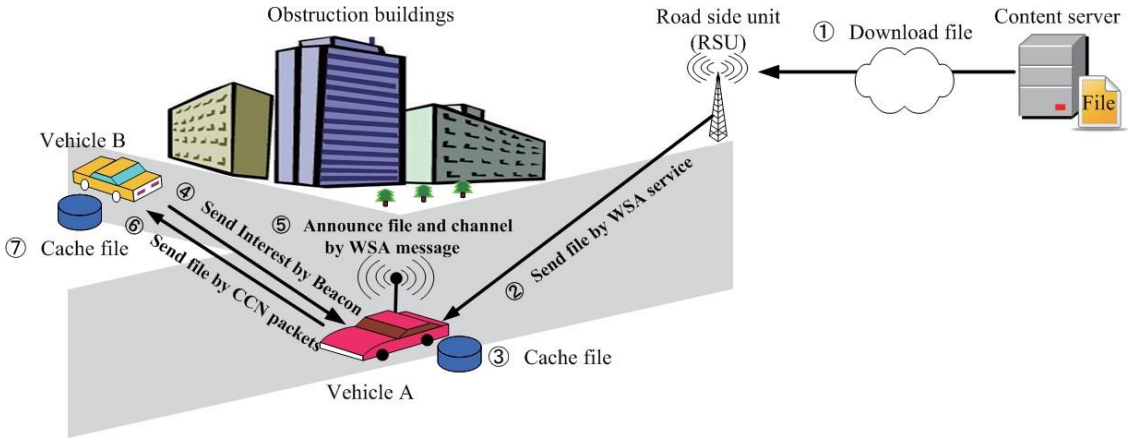

Fig. 4.3. CCN-based content distribution architecture.

Safety and non-safety application are separated on different channel, which is controlled by multi-channel operations (1609.4). In PHY layer, there are one control channel (CH) and 6 service channels (SCH) are available shown in Fig. 4.4 (a).

A consensus in the industry is to send all collision avoidance safety messages on control channel 178 [47], [57]. Other six service channels have not been sufficiently used and not been exclusive for specified applications, while channels 174 and 176 are reserved for medium power application, which is responding to IP packets transmission [46], [57]. To avoid channel interference, in this paper we suggest Channel 174 is allocated to IP packets for R2V communication, Channel 176 is allocated to CCN packets for V2V communication.

The WSA is a management message. The WSA includes information offered in an area, for example, traffic alert, tolling, navigation, entertainment, and internet access. WSAs are sent on the CCH during the CCH interval, the services that a WSA advertises is offered on SCHs. Service type, service offering channel and other connection parameters are carried in WSA message [57]. Although most of service is provided by RSUs, a vehicle could also send a WSA [57], thus this provides a possibility for advertising its content from a vehicle for V2V communication. This means both RSUs and vehicles can broadcast WSAs for announcing service offerings including content name and corresponding service channels.

If SCH 174 is designated for IP packets and SCH 176 is designated for CCN packets, the channel information can be carried in a WSA message. Figure 4.4 (b) shows the format of WSA [57], in the optional field, Service Info and Channel Info can be modified for suiting the proposed scheme. In Service Info field, a service type and corresponding service channels are indicated: IP service (IP address) or CCN service (content name). Service Info field is linked to Channel Info field by the Channel Index [57]. If the service is IP service, the Channel Number is set to 174; if the service is CCN, the Channel Number is set to 176. Thereby service advertisement including content name and channel number could be achieved.

4.6.2 Piggyback Content Name on a Beacon Acting as an Interest Message

An Interest occurs in vehicle-to-vehicle communication for requesting content files. We need to choose a suitable Interest's substitute in DSRC specifications.

WSMP is specifically designed for the short message exchange in vehicular networks. On one hand, WSMP packets can carry high-priority safety message, traffic and road message, or beacon frame. WSMP packets can be directly exchanged by WAVE devices without IP overhead both on CCH and SCH [57]. Beacons are one-hop broadcasted short message whereby all vehicles send status information about the vehicle type, position, speed, and direction.

On the other hand, broadcast is one of options for Interest routing in dynamic vehicular network. Beacon enables to satisfy either the V2V communication requirement or the broadcast characteristic so that beacon can be a substitute of Interest in vehicular CCN.

Thereby we design the Interest message by modifying the beacon frame. The format of beacon frame is shown in Fig. 4.5 [77]. In the frame body the last field is Vendor-Specific element, the content name of an Interest could be piggybacked onto the last field of frame body, while being fully compliant with the 802.11p/WAV E specification. A beacon piggybacked by a content name acts as an Interest of CCNP service.

Piggybacked beacon as an Interest is sent to vehicles, which is supported by WSMP. If Interest receiver fortunately cache this content, the content file is sent to the subscriber, which is supported by CCNP service.

4.6.3 Cache Strategy in Vehicular CCN

Although there are sufficient cache strategies proposed for CCN in previous works, e.g., LCD (leave copy down), MCD (move copy down), Prob (copy with probability), Prob Cache (a weighted probability cache) and so on [78]– [82], due to VANETs characteristic of mobility, short-lived and intermittent connectivity, caching strategy has to be uncoordinated, distributed and enhanced. A cache strategy called leave copy everywhere (LCE) for every vehicle is borrowed for V2V communication in our work. LCE can expand coverage range of transmission and decrease relay times. The operation of LCE in vehicular network will be described in next section.

Besides, Least Frequently Used (LFU) replacement algorithm is suggested to run in all caches. In metropolitan areas, LFU algorithm in caches is reasonable according to link popularity [80]. In our simulation, since only one file is assumed to be distribution, LFU algorithm is not included in simulations.

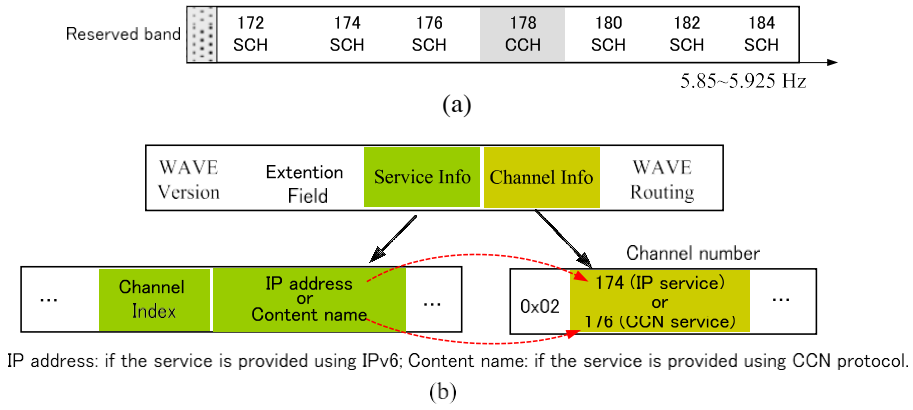

Fig. 4.4. Modified WSA message (a) the DSRC channel allocation in U.S and (b) WSA message format.

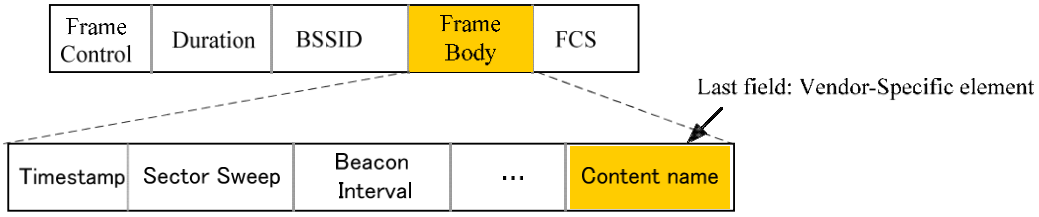

Fig. 4.5. Beacon frame format and its modification as an Interest.

4.7 Application Descriptions of Proposed and Existing

Application cases corresponding to the proposed CCN- based scheme and existing DSRC-based scheme respectively for comparison are depicted in Fig. 4.6 and Fig. 4.7. The target is all of cars capture a file that is initially placed in a content server.

4.7.1 Case-A: Proposed CCN-Based Scheme

In the case of CCN-based scheme shown in Fig. 4.6, cars are sorted into two groups according to the derivation of the file from R2V or V2V. First, WSA service offers a file to a fraction of cars from RSU. These cars belong to Group 1. Secondly, other cars acquire this file from cars in Group 1, these cars belong to Group 2. The cache policy of Group 1 shown in (a): after node 1 downloads a file from RSU, caches this file. The cache policy of Group 2 is shown in (b) and (c). The nodes in Group 2 capture the file by two ways. One is shown in (b): node 1 catches the file from node 2 of Group1, caches this file. Another shown in (c) is, node 1 requests the file via relay node 2 of Group2 to node 3 of Group1. On the back way, this file is cached in every node. Above operations called leave copy every-where are repeated for every node.

4.7.2 Case-B: Legacy DSRC-Based Scheme

In the case of DSRC-based scheme shown in Fig. 4.7, WSA service offers a file to cars by broadcast from RSU via content-server. Cars obtain the file only from RSU. All of vehicles capture files through R2V communication. Single- RSU and five-RSU deployments are shown in Fig. 4.7 (a) and (b) respectively, which is used to estimate the multi-RSU deployment. The maximum number of a reasonable RSU deployment is 5 in the experimental area, which is decided by the radio coverage range defined in DSRC specifications. The furthermore explanation will be followed in the Sect. 6.1. In the next section, the applications of case-A and case- B will be simulated in various scenarios.

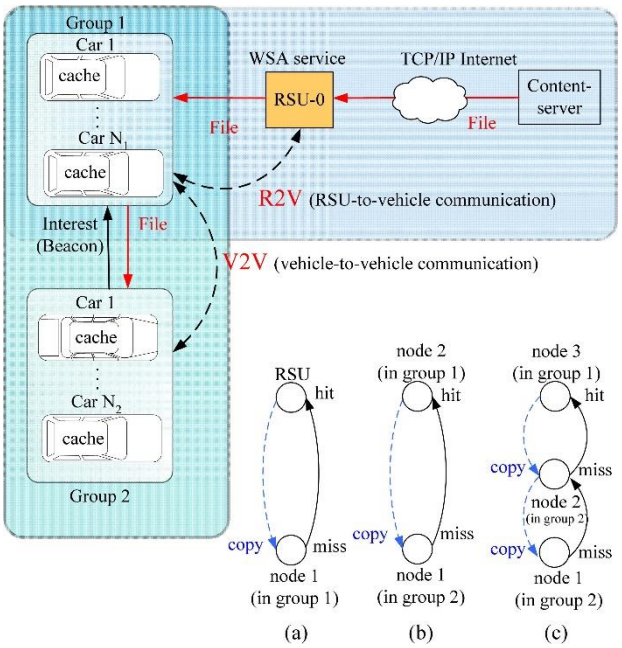

Fig. 4.6. Proposed scheme with cache strategy of Case-A.

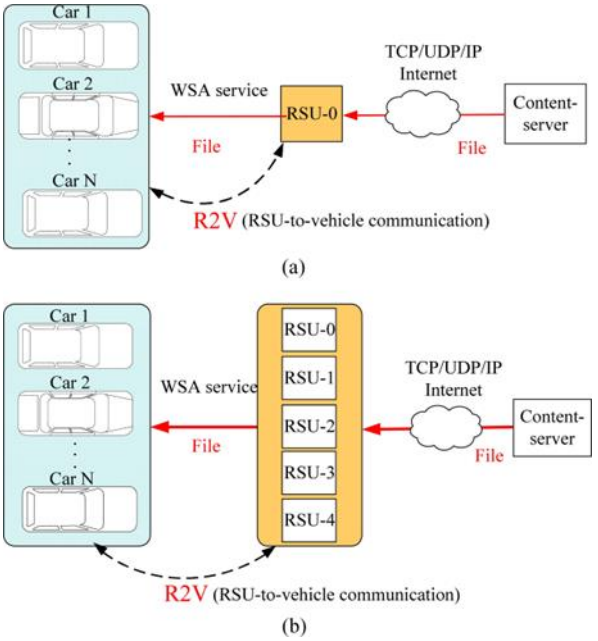

Fig. 4.7. DSRC-based scheme of Case-B with (a) single-RSU deployment and (b) multi-RSU deployment.

4.8 Simulation-Based Validation

Proposed CCN-based scheme is compared to existing DSRC-based scheme in the different scenarios for evaluating the performance of content distribution. Cars are going into a metropolitan area called Sannomiya of Kobe in Japan showed in Fig. 4.8 (a), which is a realistic traffic map downloaded from OpenStreetMap [38]. If zooming in the central location, the vehicle movements can be observed in Fig. 4.8 (b). The simulation is implemented by OMNeT++ 4.4.1 (network simulator) [84], combining Veins 3.0 frame- work (vehicular network simulator) [40] and SUMO 0.21.0 (urban mobility simulator) [86], in which IEEE 802.11p protocol stack and signal attenuation caused by obstacles are included [85]. Besides, we designed software to generate the traffic routes for every car, so the reasonable and realistic traffics could be able to be provided. This traffic system enables the simulation results more reliable for validation.

One file of 2.92 MB will be distributed to cars from RSU. The simulation traffic area is scoped within 1.06 ×1.2 km2. A file of 2.92 MB is divided into 2000 packets to dis- tribute to cars. All of cars are assumed to be DSRC-CCN- equipped in case-A and DSRC-equipped in case-B. With different traffic loads (200 and 800 cars) and different RSU deployment (1 or 5), cars will receive the file within 900 seconds simulation time. The packet delivery ratio as a main metric is evaluated.

4.8.1 Traffic Load of Simulation Scenarios

The low traffic load and the high traffic load are respectively provided for two schemes for evaluating the effectivity and robustness of proposed scheme. For the high traffic density, in the same lane, the distance between two adjacent vehicles is around 10 meters [50]. According to this estimation, 200 cars and 800 cars are assumed to be a low and a high traffic loads respectively. The simulation scenarios are as follows:

1. 200 cars of low traffic load are going into a metropolitan area in both schemes.

2. 800 cars of high traffic load are going into a metropolitan area in both of schemes.

4.8.2 Road-Side Unit (RSU) Deployment

The RSU deployment is shown in Fig. 4.8 (c):

1. The RSU named RSU-0 is deployed in simulation scenario for both schemes. When the RSU-0 shown in Fig. 8 (c) is deployed in two schemes, that located in the center of the traffic area of ABCD.

2. Five RSUs named RSU-0∼4 are deployed only in existing DSRC-based scheme to observe

how much improvement that multi-RSU deployment works.

One RSU typically can reach with a single hop distance [87]. DSRC messages reach their destinations in a single hop [57]. The single-hop distance is decided by DSRC- equipped devices. DSRC defines four classes of device, labeled A-D, each class is associated with a maximum al- lowed transmit power at the antenna and a desired transmission range [57]. Device participating in safety is normally in class C associated with a theoretical transmission range of 400 meters with no fading or interference [58], [59]. Considering harsh environmental factors and bigger TCP/UDP packet size for content delivery, the practical coverage range is reduced to 75%, approximately 300 meters [59]. Considering the higher vehicle density in the traffic center than in the edge of the downtown, five RSUs in the experimental zone of 1.06 × 1.20 km are radially deployed from the center shown in Fig. 4.8 (c).

4.8.3 File Size and Packet Number

A file of size 2.92 MB is setup to be distributed from a server to cars. This file is broken into segments to be trans- mitted. We setup MSS (maximum segment size) of 1460 bytes for TCP packet, which is in the range of typical MTU (maximum transmission unit) between 576 bytes in the Internet and 1500 bytes in Ethernet [50], [88], [89]. The typical size proposed by CCN is also 1500 bytes in packet- lever [90], [91]. Thus, in the simulation the consistent packet size could be able to be used for both TCP/UDP/IP packets and CCN packets, as well as compatibility with wireless network like Ethernet. Whereby 1500 bytes MTU is adopted, which leads to 1460 bytes (subtracting TCP/IP header) maximum segment size (MSS), so the packet number is 2000. 2000 packets are distributed from RSU to cars. Table 4.1 shows the major simulation parameters.

4.9 Simulation Results

To leverage CCN in vehicular networks will result in sophisticated amendment on DSRC.

When there are 200 cars in a scenario, the ideal total number of received packets by all of cars is 200 × 2000; it is 800 × 2000 for 800 cars. Packet delivery ratio is a metric to evaluate how many packets are received by cars.

$$\text{Packet delivery ratio} = \text{Received packets} \,/\, \text{Total packets}$$

4.9.1 Comparison in Different Traffic Load

Figure 4.9 (a) and (b) show the packet delivery ratios in 200 and 800 cars scenarios

respectively, which is corresponding to Case-A in Fig. 6 and Case-B in Fig. 4.7 (a). In both of scenarios, proposed CCN-based scheme performs outstandingly than DSRC-based scheme.

When traffic load is increased from 200 cars to 800 cars, for the proposed scheme, the packet delivery ratio still keeps 97%; the legacy scheme takes more long time to reach 67%. The proposed scheme represents stronger robustness than legacy scheme in high traffic load scenario.

4.9.2 Comparison in Different RSU Deployment

The existing DSRC scheme is deployed with 1 and 5 RSUs respectively shown in Fig. 4.10 (a) and (b). In order to observe easily, the data curve shown in Fig. 4.9 is also attached in the Fig. 4.10.

When one RSU is deployed in DSRC scheme, the performance is fade than proposed scheme in Fig. 4.10 (a). If RSU deployment is increased to 5 shown in Fig. 4.10 (b), the performance is still fade comparing with the proposed scheme despite the proposed scheme is deployed only one RSU. Besides, even though RSU deployment is increased to 5, the data delivery ratio is not so much improved because of the impact of obstacle shadow.

Above observation presents the fact that in current DSRC, although multi-RSU deployment could improve data transmission to a certain degree, its efficiency is not limitless increasing. In-network caching technique perhaps could realize more effective improvement for data transmission.

4.9.3 Evaluation on Cache Function

Furthermore, we analyzed the detailed component of packet delivery ratio, which is composed of two parts. One is con- tributed by cache nodes (V2V communication); another is contributed by RSU infrastructure (R2V communication). In the low traffic load (200 cars) shown in Fig. 4.11, 87% packets are delivered by V2V communication, which is re- lying on cache function; 13% packets are delivered by R2V communication. Similarly, in the high traffic load (800 cars), 89% packets are delivered in V2V communication, only 11% packets are delivered from RSU. These results mean vehicle-to-vehicle communication supported by cache nodes is much active than RSU-to-vehicle communication supported by RSU. The cache nodes dominate the packet delivery.

Thereby we conclude the proposed CCN-based scheme performs stronger robustness and stability even in both of the low and high traffic loads scenarios. Besides, though its RSU deployment can be reduced to the minimum (only one), it enables to achieve high packet delivery ratio because in-network caching participates in most of packet delivery process.

4.10 Conclusion

A rich set of vehicular applications can be envisioned such as safety and non-safety applications. Though the primary motivation for deploying DSRC is to enable collision prevention, it can also be used for more general entertainment, commercial, and social purposes of non-safety application beyond the initial collision avoidance. In this research, we concentrate on a particular application of content distribution. We reviewed the related reference literatures, which enlightens our inspiration. We analyze DSRC protocol stack and Content-Centric Networking, whereby proposed a CCN-based scheme that adds CCN framework into DSRC standard for facilitating content propagation in vehicular networks. CCN framework is used for vehicle-to-vehicle communication; current DSRC standard is still served to RSU-to-vehicle communication.

Besides, we demonstrate the feasibility that a CCN framework might be working on the top of DSRC standard relying on modifying beacon and WSA message acting as Interest and Advertisement message of CCN. Certainly, to leverage CCN paradigm in vehicular networks could result in sophisticated amendment on DSRC standard, that means quantity of IEEE specifications and frames format might be involved in, however, in this research just limited and basic efforts are done. In addition, according to the characteristic of vehicular networks, hierarchical structure of naming, on-path routing, Leave Copy Everywhere of cache strategy, and Least Frequently Used algorithm are borrowed for vehicular CCN paradigm.

Proposed CCN-based scheme is compared to current DSRC-based scheme in various scenarios with massive cars traffic for evaluating its performance. The simulation tools of OMNeT++ & Veins & SUMO, associating with CCN protocol and realistic traffic routes generated by our simulation platform, enable a reliable validation. Simulation results demonstrate the proposed CCN-based scheme performs stronger robustness and stability in both of low and high traffic loads scenarios. Additionally, the RSU deployment can reduced to the minimum, simultaneously which enable to achieve high packet delivery ratio because CCN framework participates in most of packet delivery process so as to effectively facilitate data delivery for DSRC IP service.

Vehicular Content-Centric Networking opens a prospective direction for disseminating contents in metropolitan areas. The efforts to develop DSRC standards are still underway in different regions and countries, so we expect our research work could provide references for DSRC standardization that will be implemented in the future fascinating vehicular networks.

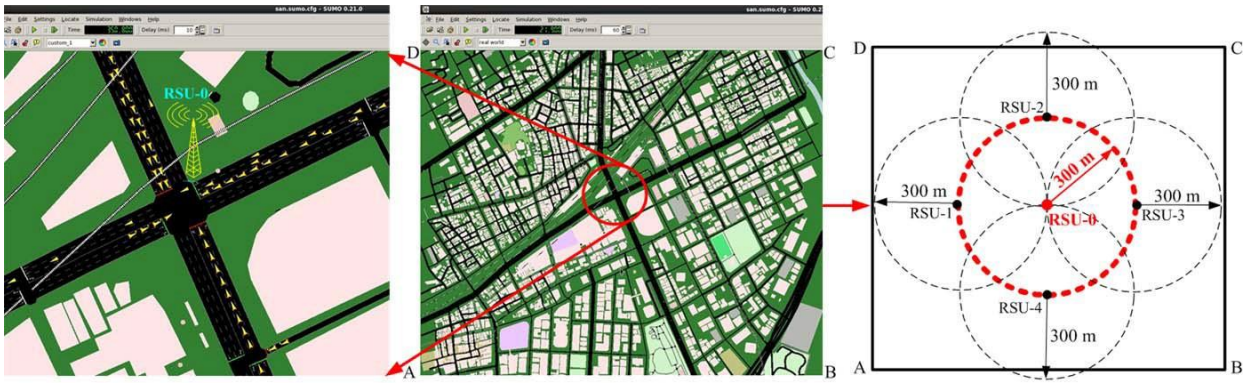

Fig. 4.8. Simulation scenario: (a) city scenario (Sannomiya of Kobe, Japan), (b) cars movements, and (c) RSU deployments.

TABLE 4.1: Simulation parameters

Parameter	Value	Parameter	Value
Location	Latitude: 34.6882~6978; Longitude: 135.1864~2017	Beacon interval as Interest	1 sec.
Vehicle number	200 (low traffic load) & 800 (high traffic load)	Broadcast interval for RSU	0.01 sec.
RSU number	1 & 5	Broadcast interval for vehicles	0.05 sec.
File size	2.92 MB	Simulation time	900 sec.
Packet number	2000	Max. Transmission power	20 mW
MSS of TCP/IP/UDP packet	1460 bytes	MAC Bit Rate	18 Mbit/s
MTU	1500 bytes	Transmission range	300 meters
On-path routing	Broadcast	Vehicle speed	0~60 km/h

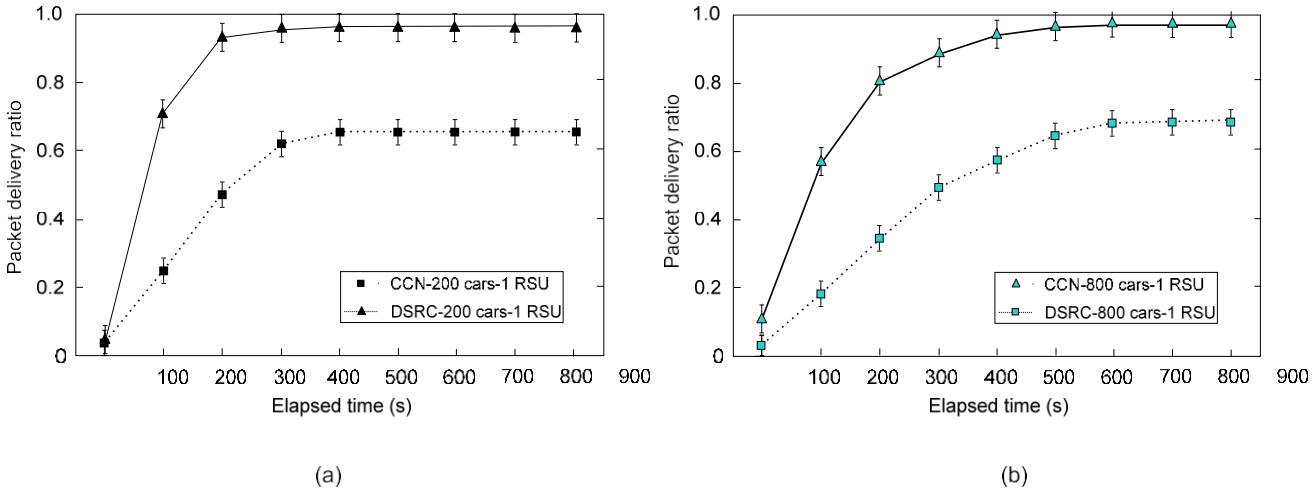

Fig. 4.9. Packet delivery ratios in the scenarios of (a) low traffic load (b) high traffic load

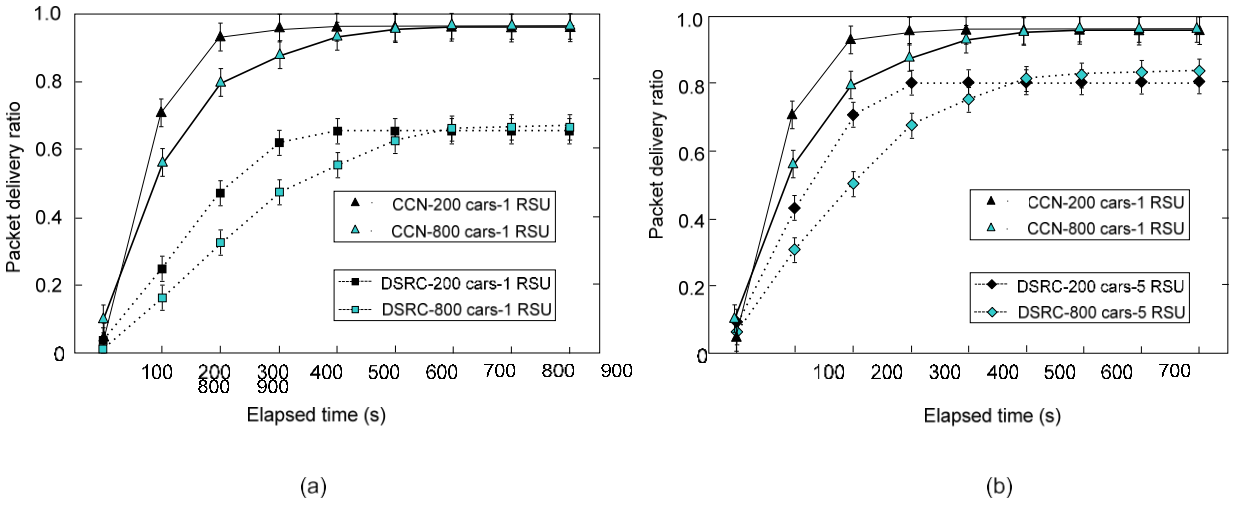

Fig. 4.10. Packet delivery ratios in the scenarios of (a) 1 RSU deployment and (b) 5 RSUs deployment.

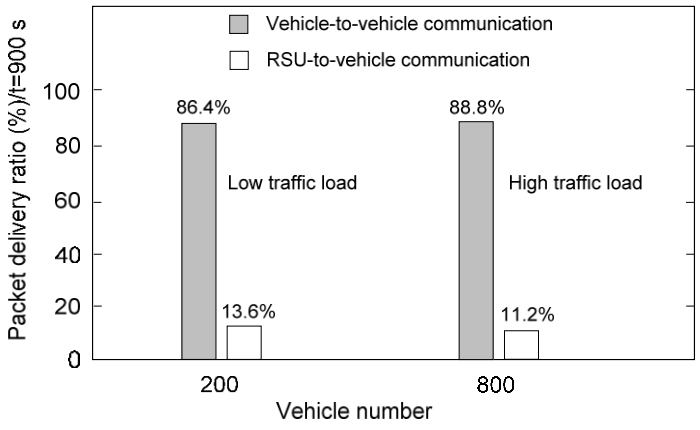

Fig. 4.11. Packet delivery ratios achieved by V2V and R2V communications in the low and high traffic load.

Chapter 5

A PKG-Node distributed Identity-Based Encryption Scheme in CCN Vehicular Network

5.1 Abstract

In public key authentication systems, Identity-Based Encryption (IBE) is recognized as a relatively better solution for vehicular networks compared to Public Key Infrastructure (PKI). However, the key escrow issue is a bottleneck for IBE. This study reviews and compares various solutions to the IBE key escrow problem, ultimately selecting a practical solution tailored for CCN-based vehicular networks. Specifically, considering the unique characteristics of dynamic nodes, including their strong mobility and timeliness, a PKG-Node distributed algorithm based on the principles of BF-IBE and D-PKG ideas is tailored for CCN vehicular networks. The algorithmic process is embedded into specific RSU-to-vehicle and vehicle-to-vehicle application scenarios. Additionally, a timeliness strategy for public keys based on vehicle identity IDs is integrated to mitigate key leakage risk. This approach assigns an expiration date to each public key, ensuring that compromised keys are only valid for a limited time.

5.2 Introduction

Vehicular networks, also known as Vehicular Ad Hoc Networks (VANETs), play a critical role in the advancement of intelligent transportation systems. These networks enable vehicles to communicate with each other and with roadside infrastructure, thereby improving traffic efficiency, safety, and overall driving experience. Ensuring secure communication in such highly dynamic and mobile environments is a significant challenge, necessitating the use of robust cryptographic techniques.

Public Key Infrastructure (PKI) has traditionally been employed as the backbone of secure communications in various network environments, including vehicular networks. PKI relies on a trusted Certificate Authority (CA) to manage public and private keys, ensuring authentication and authorization [92]. While PKI provides high levels of security and trust, the complexity of certificate management, which includes the generation, distribution, revocation, and updating of public key certificates, imposes substantial operational and cost overheads. This complexity is particularly problematic in vehicular networks, where the

dynamic nature of communication and the frequent addition of new nodes demand more efficient and flexible solutions.

Identity-Based Encryption (IBE) has emerged as a promising alternative to PKI for vehicular networks. The mathematical foundation of the IBE scheme is built on elliptic curve cryptography (ECC), which offers significant advantages in terms of key length and computational efficiency compared to mainstream RSA-based schemes [93-95]. The rigor of IBE algorithm has been strictly proven. By using user identity information, such as number plate or IP addresses, as public keys, IBE eliminates the need for public key certificates, thereby simplifying the key management process. This approach is well-suited for vehicular networks, where dynamic key generation can accommodate the frequent addition and removal of nodes. However, traditional IBE systems face the key escrow problem, wherein the central Private Key Generator (PKG) holds significant power, posing a risk of a single point of failure and potential privacy issues.

To address these challenges, various enhancements to IBE have been attempted in some literatures, focusing on mitigating the key escrow problem [96-97]. These enhancements include Distributed Private Key Generation (D-PKG), key splitting, and escrow-free encryption. D-PKG involves multiple independent nodes jointly generating and managing private keys, thereby distributing trust and reducing the risk associated with a single PKG [98-100]. Key splitting divides the master key into multiple parts stored across different PKGs, requiring collaboration to reconstruct the master key and enhancing security. Escrow-free encryption aims to design algorithms that ensure PKGs cannot directly decrypt user ciphertexts, even with access to the master key, thereby enhancing privacy protection.

This study reviews and compares various solutions to the IBE key escrow problem, ultimately selecting a practical solution tailored for Content-Centric Networking (CCN) based vehicular networks. Considering the unique characteristics of vehicular network nodes, including their strong mobility and timeliness, this research proposes a PKG-Node distributed algorithm based on the principles of Boneh-Franklin Identity-Based Encryption (BF-IBE) [93-97] and Distributed Private Key Generator (D-PKG) [98-101]. The proposed algorithm aims to enhance the security and reliability of vehicular networks by addressing the key escrow problem while accommodating the dynamic nature of vehicular communication.

The proposed PKG-Node distributed algorithm leverages the mathematical foundations of BF-IBE and D-PKG to create a robust and scalable solution for CCN vehicular networks. By distributing the key generation process between the PKG and individual nodes, the algorithm reduces the risk of a single point of failure and enhances the overall security of the network. Additionally, a timeliness strategy for public keys based on vehicle identity IDs is introduced, assigning expiration dates to mitigate key leakage risks. This strategy ensures that compromised keys have limited utility, thereby enhancing the overall security of the network.

To demonstrate the practical application of the proposed algorithm, the study embeds the algorithmic process into specific RSU-to-vehicle and vehicle-to-vehicle communication scenarios. These application scenarios illustrate how the algorithm facilitates secure interactions between roadside units (RSUs) and vehicles, as well as between individual vehicles. By providing a comprehensive overview of the algorithm's integration within CCN vehicular networks, this research highlights its potential to enhance the security, scalability, and reliability of dynamic vehicular communication environments.

In conclusion, this study contributes to the ongoing development of secure vehicular networks by proposing a practical and mathematically robust solution to the key escrow problem in IBE. The PKG-Node distributed algorithm, tailored for CCN vehicular networks, offers a promising approach to enhancing the security and efficiency of vehicular communication, thereby supporting the advancement of intelligent transportation systems.

5.3 Background and Our Contributions

5.3.1 A Review of IBE and PKI

The security of information encryption no longer relies on algorithms themselves, but rather on making them public and focusing on computational complexity. Similarly, the analysis of password security has undergone a similar process. The security of widely used and researched PKI (Public Key Infrastructure) and IBE (Identity-Based Encryption) systems is also based on publicly known algorithms and computational complexity. Their complexity lies in mathematical problems such as large integer factorization and discrete logarithms [102-103].

In vehicular networks (VANETs), Identity-Based Encryption (IBE) and Public Key Infrastructure (PKI) are two primary cryptographic and authentication techniques. PKI is a widely used cryptographic and authentication technique in various network environments. Its core is the management of public and private keys by a Certificate Authority (CA). The application of PKI in vehicular networks includes authentication and authorization, encrypted communication. PKI offers high levels of security and trust through strict certificate management and authentication mechanisms, and widely adopted in various network environments, with mature standards and good compatibility. But due to complex certificate management, PKI requires the generation, distribution, revocation, and updating of public key certificates, making the management process complex and costly. Besides, it requires storing quantity of public key certificates and corresponding revocation lists (CRLs), so it performs complex certificate validation and management operations.

On the other hand, IBE uses user identity information (such as number plate or IP addresses) as public keys, eliminating the need to generate and distribute public key certificates so that it significantly simplifies the key management process. Private keys can be dynamically generated as needed, suitable for vehicular networks where frequent communication and dynamic addition of new nodes are common. IBE private keys can be dynamically generated as needed. IBE's dynamic key generation mechanism is well-suited for the frequent addition and removal of nodes, which is common in vehicular networks. For a large of nodes in vehicular networks, traditional certificate management systems could be complex and costly. IBE simplifies the key management process, reducing overall management costs. Besides, by encrypting vehicle identity information, IBE protects vehicle privacy, preventing identity leakage. Though IBE simplifies key management and is well-suited for dynamic and high-frequency communication environments but relies heavily on a central Private Key Generation (PKG), which cause private key escrow vulnerability that could be a single point of failure.

Targeting to solve the key escrow problem in IBE, some practical deployments in vehicular networks and other applications are proposed to mitigate the risks associated with a single

Private Key Generation Center (PKG), such as distributed key generation (DKG), key splitting, escrow-free encryption and so on. DKG involves multiple independent nodes jointly generating and managing private keys, thus reducing the risk of a single PKG having full control. While it enhances security and distributes trust, it also introduces complexity in implementation and increases communication overhead among nodes. Key splitting divides the master key into multiple parts, each stored in different PKGs. This approach increases security by requiring multiple PKGs to reconstruct the master key and is relatively simpler to implement than fully distributed systems. However, it still involves partial trust issues and requires effective coordination among PKGs especially in vehicular network. Escrow-free encryption involves designing new encryption algorithms that ensure the PKGs cannot directly decrypt users' ciphertexts, even if it possesses the master key and fundamentally addresses the key escrow problem and enhances privacy protection. However, it is challenging to design and implement these new algorithms, and they may introduce additional computational and communication costs.

In our research, we also address to propose practical deployments in CCN based vehicular networks for improving private key escrow vulnerability, besides private key leakage risk.

5.3.2 Our contribution

1. A Review of IBE

IBE (Identity-Based Encryption) represents an advancement in the field of cryptography, offering a streamlined approach to public key management by using a user's unique identity as the public key. This review aims to provide a comprehensive overview of IBE, exploring its foundational principles, inherent challenges, and the various solutions developed to address these challenges. The primary objective of this review is to elucidate the practical applications of IBE, particularly in dynamic and security-sensitive environments in vehicular networks. By examining the current state of IBE technology, including advancements in addressing the key escrow problem and other security concerns, this review seeks to inform and guide future research and implementation efforts. Ultimately, this review aspires to present a scheme to simplify cryptographic processes while ensuring robust security in CCN vehicular network.

2. Proposed PKG-Node distributed IBE scheme integration with CCN vehicular Network

Considering the unique characteristics of dynamic nodes, including their strong mobility and timeliness, a PKG-Node distributed IBE (P-N-IBE) algorithm based on the principles of BF-IBE and D-PKG ideas is tailored for CCN vehicular networks. The algorithmic process is embedded into specific RSU-to-vehicle and vehicle-to-vehicle application scenarios. Furthermore, the integration framework of the P-N-IBE scheme within vehicular networks, is illustrated how it facilitates secure interactions between roadside infrastructure and vehicles,

as well as the framework for vehicle-vehicle communication. By presenting the mathematical underpinnings and algorithmic steps, aiming to provide a clear understanding of how the P-N-IBE scheme operates. This includes key generation, encryption, and decryption processes, highlighting the collaborative efforts of multiple nodes to enhance security and trust. Overall, this section aims to provide a comprehensive overview of the P-N-IBE scheme's theoretical foundations and practical implementation in CCN vehicular networks, emphasizing its potential to enhance security and reliability in these dynamic environments.

3. Timeliness Strategy for Public Keys Based on Vehicle Identity IDs for Mitigating Key Leakage

To address reducing the risk of attackers maliciously stealing data and compromising the system, this research proposes a timeliness strategy for public keys based on vehicle identity IDs to mitigate these risks. The proposed timeliness strategy involves assigning an expiration date or validity period to each public key generated from a vehicle's identity ID. This ensures that even if a private key is compromised, its utility is limited to a specific time frame, after which it becomes invalid. By periodically updating and rotating keys, the system can significantly reduce the window of opportunity for attackers to exploit leaked keys.

5.4 A Review of IBE

For IBE encryption algorithms, elliptic curve cryptography (ECC) is utilized. Compared to RSA, assuming both algorithms are at the same security level, the key length for ECC is 163 bytes, while the key length for RSA is 1024 bytes. This shows that the key length for ECC is approximately 84% shorter than that of RSA [104-105]. Therefore, using ECC encryption will save a significant amount of storage space and computation time, making its application in constrained vehicular networks highly significant. Currently, most standard applications do not support IBE encryption. However, extensive research literature indicates that pseudo-RSA digital certificates can serve as a substitute for implementing IBE schemes. This provides support for deploying IBE in practical scenarios.

IBE schemes have garnered significant attention and development in recent years. The most prominent IBE schemes are BF-IBE, D-PKG, Partial Double Encryption, and Attribute-Based Encryption (ABE). Below is a summary of their application status. These insights can help us to shape a research direction in CCN vehicular network.

5.4.1 BF-IBE

The BF-IBE scheme, proposed by Dan Boneh and Matthew Franklin in 2001, is one of the pioneering IBE systems [92]. It leverages bilinear pairings on elliptic curves to achieve encryption and decryption. The scheme has been extensively studied for its mathematical foundation and security properties. BF-IBE has been applied in various domains requiring secure communication and efficient key management, particularly in environments where a PKI is impractical. While BF-IBE is a pioneering and influential identity-based encryption

scheme, it has several weaknesses called key escrow problem, that limit its practical deployment especially in vehicular network. BF-IBE centralized control by the PKG raises significant trust and security concerns in an open vehicular network environment. The following schemes provide solutions insights for key escrow problem.

5.4.2 D-PKG

D-PKG (Distributed Private Key Generator) addresses the key escrow problem in traditional IBE systems by distributing the role of PKG across multiple authorities. This approach enhances security by ensuring that no single entity has complete control over the key generation process. D-PKG is well-suited for decentralized systems where trust is distributed among multiple entities. Applications include federated identity management, secure multi-party communications, and blockchain-based systems [98-101]. The distributed nature of D-PKG makes it particularly attractive for environments requiring high resilience and security, such as critical infrastructure protection and collaborative platforms.

While D-PKG schemes offer significant advantages in enhancing security and reducing reliance on a single PKG, they face several challenges in dynamic vehicular networks. The complexity of coordination, scalability issues, fault tolerance, security risks from compromised nodes, and communication overhead are notable weaknesses that need to be addressed for effective deployment in such environments. Future research should focus on developing more simple, robust, efficient, and scalable solutions to overcome these challenges.

5.4.3 Partial Double Encryption

Partial Double Encryption combines IBE with traditional public key encryption methods to enhance security and reduce reliance on a single cryptographic assumption [108]. This hybrid approach aims to leverage the strengths of both IBE and PKG. This scheme is applied in high-security environments where multi-layered encryption is essential. Examples include financial transactions, secure communications in military networks, and protecting sensitive data in healthcare systems. By using dual encryption layers, Partial Double Encryption mitigates the risk of single-point cryptographic failures. However, it faces several weaknesses, especially in dynamic vehicular networks:

Computational Overhead: Increased computational demands can degrade performance and increase energy consumption.

Increased Latency: The dual encryption process introduces additional latency, impacting real-time communication.

Key Management Complexity: Managing multiple keys adds complexity and operational overhead.

Security Trade-offs: The overall security depends on the robustness of both encryption

methods, introducing potential vulnerabilities.

Bandwidth Consumption: Larger ciphertext sizes result in higher bandwidth consumption, contributing to network congestion and transmission costs.

5.4.4 Attribute Based Encryption

ABE extends the concept of IBE by allowing encryption and decryption based on user attributes rather than a unique identity. This enables fine-grained access control and is highly flexible for complex access policies. ABE schemes can be categorized into Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE), each providing different methods for policy enforcement [109-110]. ABE is widely used in environments that require sophisticated access control, such as cloud computing, secure data sharing, and healthcare information systems. Its ability to enforce access policies based on user attributes makes it suitable for dynamic and large-scale systems. While Attribute-Based Encryption (ABE) offers fine-grained access control and flexibility, its application in dynamic vehicular networks presents several weaknesses:

Computational Overhead: High computational demands can lead to performance and energy consumption issues.

Key Management and Attribute Revocation: Efficiently managing and revoking attributes is complex and can cause scalability issues.

Latency and Real-Time Communication: High latency from complex operations affects real-time data transmission.

Policy Management Complexity: Managing detailed access policies adds administrative burden and reduces flexibility.

Based on the various improved IBE schemes mentioned above, this study proposes a lightweight solution based on BF-IBE and D-PKG idea to address the key escrow vulnerability. This solution is designed to be deployed in R2V (Roadside-to-Vehicle) and V2V (Vehicle-to-Vehicle) application scenarios. The basic idea of this scheme is to use the PKG (Private Key Generator) and one vehicle node as key escrow nodes. Compared to the above schemes, this approach strikes a good balance between computational load and complexity. This paper will not detail the rigorous mathematical derivation (because some references are listed), focus on describing the computational processes and the deployment structure within CCN vehicular network.

5.5 Proposed P-N-IBE Scheme Leveraged in CCN Vehicular Network to Solve Private Key Custody Vulnerabilities

5.5.1 An Overview of BF-IBE Encryption Algorithm

The Identity-Based Encryption (IBE) algorithm, which is based on identity encryption, was first proposed by Shamir [93]. This algorithm essentially falls under the category of public key encryption. In this cryptographic system, user specific data, such as number plate, can be used as the encryption public key.

1. System Initialization : Input the security parameters, and have the Private Key Generator (PKG) run the algorithm to generate the system parameters <params> and the master secret key s. The generated system parameters include the master public key and plaintext message space, among other data. The system parameters are made public to the users, while the master secret key s is privately kept by the PKG.

2. Key Extract : Input the identity ID, public parameters <params>, and master secret key s. Run the key extraction algorithm to generate the private key d_{ID} for the user with the specified identity ID, return the corresponding private key. The identity ID is directly used as the public key.

3. Plaintext Encryption : Input the identity ID, system parameters <params>, and plaintext message M. Run the encryption algorithm to generate the ciphertext C.

4. Ciphertext Decryption : Input the ciphertext C, the user's identity ID, the private key d_{ID} corresponding to the ID, and the system parameters params\text{params}params. Run the decryption algorithm; if successful, the output will be the plaintext message M. Otherwise, the decryption will failure.

The algorithm details are shown in Figure 5.1.

5.5.2 Proposed P-N-IBE Scheme for CCN Vehicular Network

To address the key escrow problem, it is desired that IBE no longer relies solely on the PKG for private key generation, or IBE private keys are no longer formed by cooperation among multiple dynamic nodes. Considering the instability and high-speed transience in the dynamic environment of vehicular networks, we propose a compromise solution: a distributed key escrow scheme involving collaboration between one PKG and one node. The mathematical derivation of elliptic curve bilinear mappings for distributed IBE is well-documented in the literature and will not be detailed here, otherwise focuses on the basic algorithmic process [93-96,101-105]. In the key generation phase, the PKG is responsible for generating the PKG user private key, while the node is responsible for generating the node private key, with each private key being kept separately in PKG and nodes. Due to the design of the algorithm involving the private keys, the decryption process requires both types of private keys to decrypt the ciphertext. Specifically, the process is as follows: First, the node performs an initial decryption using the PKG private key controlled by the PKG. Then, the node performs further decryption using its own private key called node private key. The final plaintext is

then computed. The process includes four phases:

1. System Initialization: Input the security parameters, and Private Key Generator (PKG) run the algorithm to generate the system parameters <params> and the master secret key s. The system parameters <params> are public, while s is kept secret by the PKG as the master private key. The master public key s is computed as $P_{pub} = sP$. The plaintext space is chosen as $\mathcal{M} = \{0,1\}^*$, and the ciphertext space is $\mathcal{C} = \mathbb{G} \times \{0,1\}^*$. The system public parameters are then output, params =$\langle \mathbb{G}, \mathbb{G}_T, q, e, n, P, P_{pub}, H_1, H_2, H_3, H_4 \rangle$.

2. Key Extract**:** Input the identity ID, public parameters <params>, and master secret key s. Run the key extraction algorithm to generate the private key $d_{ID1,}$ and the node private key d_{ID2}, and the node public key P_{id}. The parameters generated by the key extraction algorithm are shown in the table below. The private key d_{ID1} is kept secret by the PKG, the node private key d_{ID2} is kept secret by the node, and the node public key P_{id} is made public.

3. Plaintext Encryption : Input the parameters <params> and the node identity ID, system parameters <params>, and plaintext message M. Run the encryption algorithm to generate the ciphertext C.

4. Ciphertext Decryption : Input <params>, ciphertext C, and private key of the node identified by ID. The node first performs decryption using the PKG user private key d_{ID1}, followed by further decryption using the node private key d_{ID2}. This process ultimately recovers the plaintext message M.

The algorithm details are shown in flowchart in Figure 5.2 and Figure 5.3.

5.5.3 Deployment of P-N-IBE in CCN Vehicular Network

- RSU-to-Vehicle scenario: the encryption and decryption process between RSU and Alice is illustrated. When they exchange information, the step of having a third-party certification authority verify Alice's public key is eliminated. The public key used for encryption can directly use Alice's identity information, simplifying the authentication management process during encryption. Alice sends her identity data to the PKG for verification. Upon successful verification, the PKG calculates her private key based on the provided identity data and returns the private key to Alice. When RSU sends a plaintext message M, it uses the public key provided by Alice and the system parameters <params> from the PKG to encrypt the information, resulting in ciphertext C. RSU then sends the ciphertext. When Alice decrypts the ciphertext sent to her, she uses the private keys calculated by the PKG and herself to recover the plaintext message M.

- Vehicle-to-Vehicle scenario: The encryption and decryption process between Alice and Bob is illustrated. When they exchange information, the step of having a third-party

certification authority verify Bob's public key is eliminated. Bob sends his identity ID to the PKG for verification. Upon successful verification, the PKG calculates his private key based on the provided identity ID and returns the private key to Bob. When Alice sends a plaintext message M, she uses the public key provided by Bob and the system parameters <params> from the PKG to encrypt the information, resulting in ciphertext C. She then sends the ciphertext to him. He uses the private keys calculated by the PKG and himself to recover the plaintext message M.

The communication scenario is shown in Figure 5.4.

5.5.4 P-N-IBE algorithm flowchart in CCN Vehicular Network

V2V (vehicle-to-vehicle) communication scenario is treated as an example to illustrate how the algorithm operates within a CCN vehicular network. The same principles apply to RSU-to-vehicle communication. The sequence diagram is shown in figure 5.5.

5.6 Extended Identity ID with Time Strategy

The consequences of private key leakage can be severe. In a PKI system, the issue of private key leakage can be addressed through certificate revocation or revocation lists, but the maintenance costs are high. To address the problem of key updates, this paper designs a time-based strategy by adding timestamp information to the identity identifier, forming a new extended identity identifier as shown below:

<Identity ID>||<TimeStamp1 : TimeStamp2>

The extended identity identifier combined with public parameters can be used to generate a public key for encrypting data, and it corresponds to a private key for decrypting data. These key pairs and the extended identity identifier are only used within the specified time period. Therefore, the time period restricts the usage of the identity identifier and its private key. If a private key is leaked, it will only affect the data encrypted within the corresponding time period. The shorter the user-defined time period, the higher the frequency of private key updates, leading to better security. This approach can mitigate the consequences of private key leakage to a certain extent and address the issue of key revocation, with significantly lower maintenance costs compared to managing CRL revocation lists in a PKI system.

5.7 Conclusion

This study presents a comprehensive analysis and solution to the key escrow problem in Identity-Based Encryption (IBE) systems, specifically tailored for Content-Centric Networking (CCN) based vehicular networks. IBE is recognized as a more suitable solution for vehicular networks compared to Public Key Infrastructure (PKI) due to its simplified key

management processes. However, the key escrow problem, where a central Private Key Generator (PKG) holds significant power, poses a potential risk and bottleneck for IBE deployment.

To address these challenges, this research reviews and compares various enhancements to IBE, including Distributed Key Generation (DKG), key splitting, and escrow-free encryption. The study proposes a practical and mathematically robust solution: a PKG-Node distributed algorithm based on the principles of Boneh-Franklin Identity-Based Encryption (BF-IBE) and Distributed Private Key Generator (D-PKG). This solution is designed to leverage the unique characteristics of CCN vehicular network nodes, including their strong mobility and timeliness.

The proposed PKG-Node distributed encryption algorithm effectively distributes the key generation process between the PKG and individual vehicle nodes, thereby reducing the risk of a single point of failure and enhancing overall network security. Additionally, the algorithm introduces a timeliness strategy for public keys based on vehicle identity IDs, assigning expiration dates to mitigate key leakage risks. This ensures that compromised keys have limited utility, further strengthening the security framework.

The practical application of the proposed algorithm is demonstrated through specific RSU-to-vehicle and vehicle-to-vehicle communication scenarios. These scenarios illustrate how the algorithm facilitates secure interactions between roadside units (RSUs) and vehicles, as well as between individual vehicles. The detailed algorithmic process, including key generation, encryption, and decryption steps, is embedded into these application scenarios, showcasing the algorithm's integration within CCN vehicular networks.

By addressing both key escrow and key leakage vulnerabilities, this study contributes to the ongoing development of secure vehicular networks. The proposed PKG-Node distributed algorithm offers a scalable and efficient solution for enhancing the security and reliability of vehicular communication, thereby supporting the advancement of intelligent transportation systems. Future work will focus on further optimizing the algorithm to reduce computational and communication overheads, as well as exploring its deployment in real-world CCN vehicular network scenarios to validate its effectiveness and scalability.

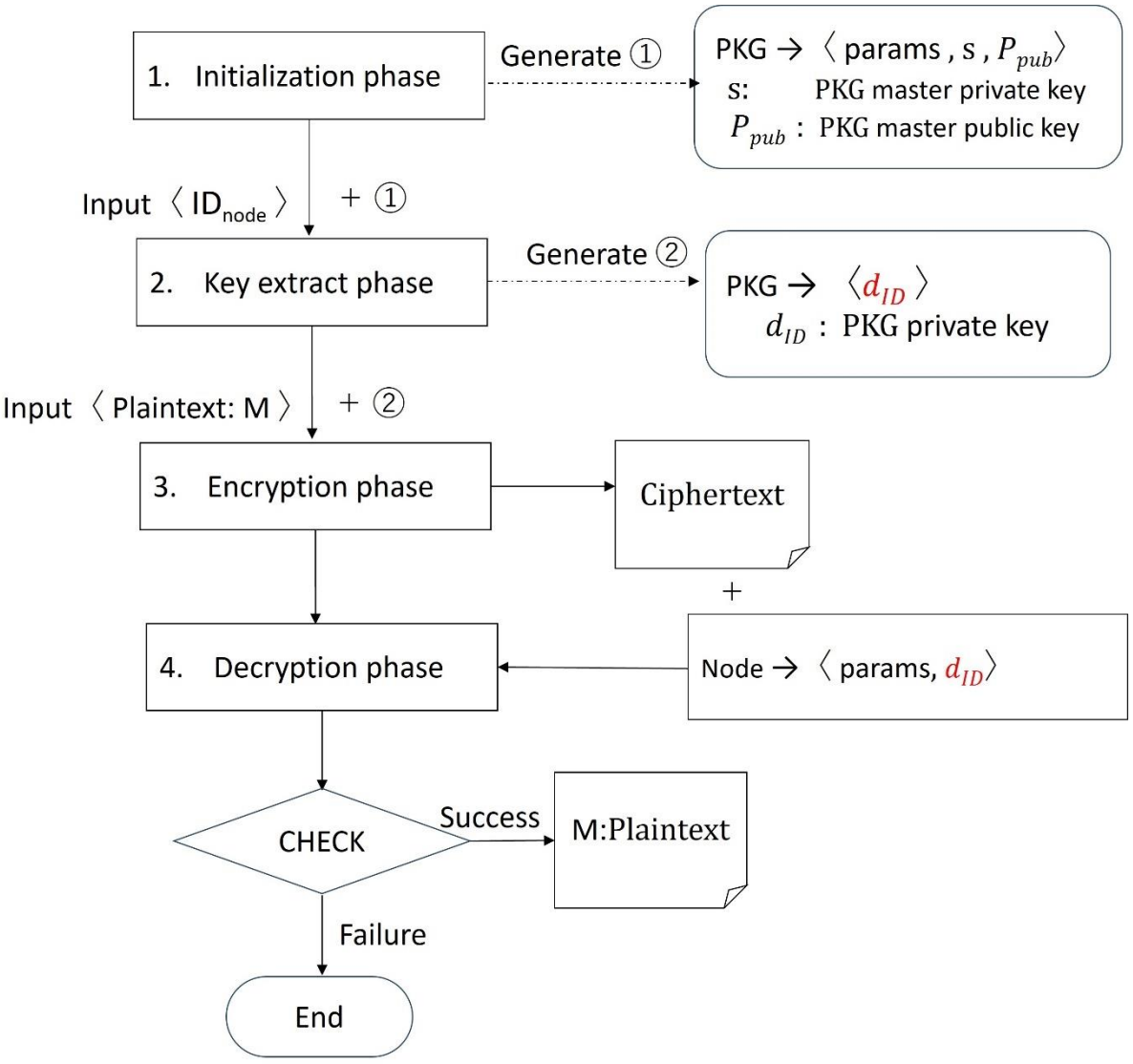

Fig. 5.1. Traditional algorithm flowchart of BF-IBE.

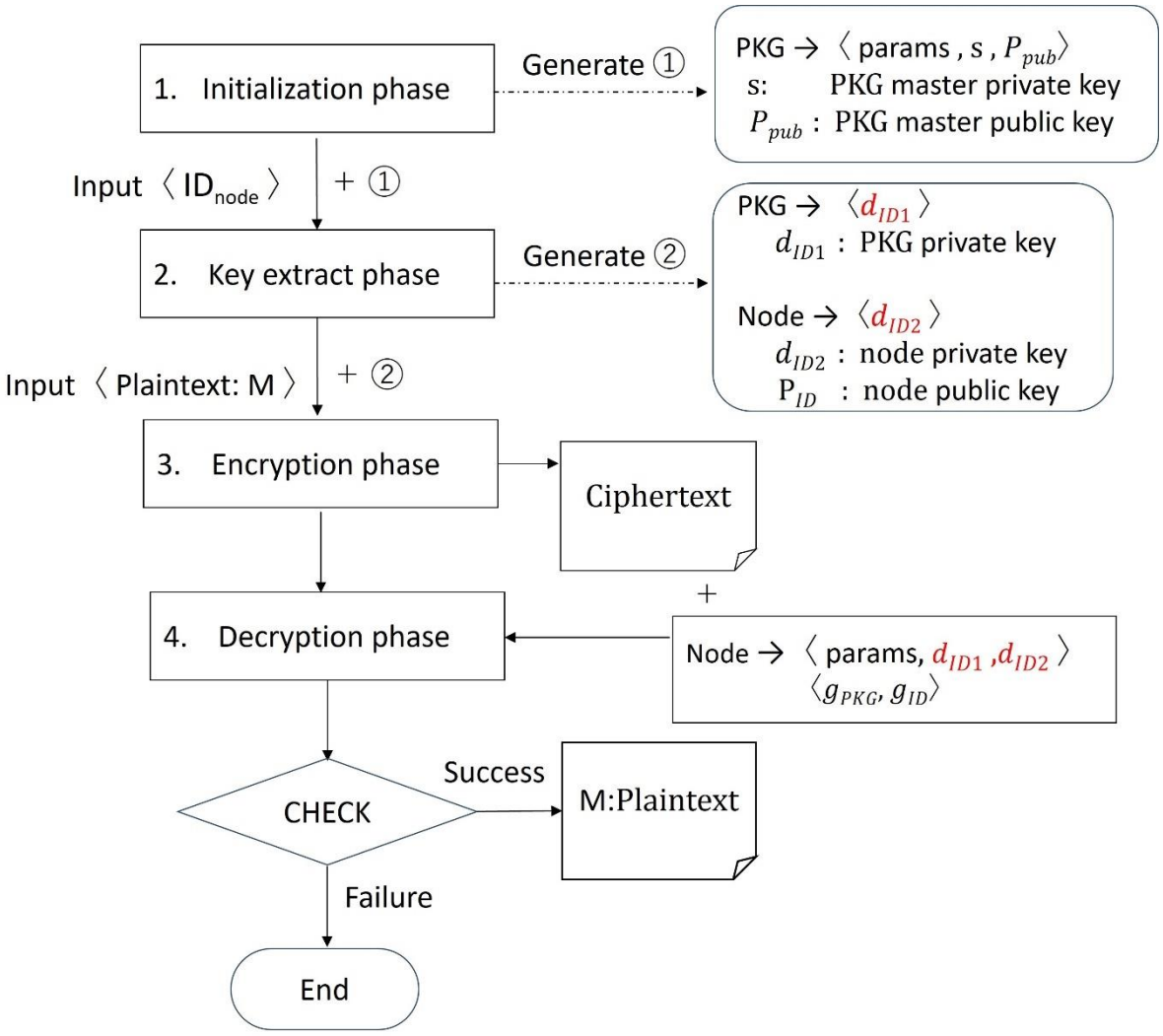

Fig. 5.2. Algorithm flowchart of P-N-IBE for CCN vehicular network.

1. System Initialization Phase

system params: $\langle \mathbb{G}, \mathbb{G}_T, q, e, P, P_{pub}, H_1, H_2, H_3, H_4 \rangle$

$\mathbb{G}$: q–order additive cyclic group (q:Prime number);

$\mathbb{G}_T$: q–order multiplicative cyclic group (q:Prime number);

$e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ (Bilinear mapping);

P: Choose a random $\mathbb{G}$'s generator;

Pick a random $s \in \mathbb{Z}q^* \leftarrow \mathbb{Z}q$: residual ring (modulo=$q$) ,

P_{pub}: $P_{pub}=sP \rightarrow \mathbb{G}^*$;

H_1 , H_2 , H_3 , H_4 : Hash function ;

$H_1 : \{0,1\}^* \rightarrow \mathbb{G}^*$; binary strings of arbitrary length

$H_2 : \mathbb{G}_T \rightarrow \{0,1\}^n$; binary strings of length n

$H_3 : \{0,1\}^n \times \{0,1\}^n \rightarrow \mathbb{Z}q^*$;

$H_4 : \{0,1\}^n \rightarrow \{0,1\}^n$;

PKG master private key: $s \in \mathbb{Z}q^*$ ← random chosen

PKG master public key: $P_{pub}=sP$

2. Key Extract phase

Step1: PKG private key: $d_{ID1} \leftarrow \langle$ params, $ID_{Alice} \rangle$

$Q_{ID}=H_1(ID) \in \mathbb{G}^*$

$d_{ID1}=sQ_{ID}$

d_{ID1} : PKG private key

P_{pub} : PKG public key

Step2: $Q_{ID}=H_1(ID) \in \mathbb{G}^*$, $x_{ID} \in \mathbb{Z}q^*$ (node random number)

$d_{ID2}=x_{ID}Q_{ID}$

$P_{ID} = \langle X_{ID}, Y_{ID} \rangle \leftarrow X_{ID}=x_{ID}P$, $Y_{ID}=x_{ID}P_{pub}$

d_{ID2} : node private key

P_{ID} : node public key

3. Encryption phase

Step1: Valid → $e(X_{ID}, P_{pub})=e(Y_{ID}, P)$

Step2: $r=H_3(\sigma, M)$ ← M: Plaintext, $\sigma \in \{0,1\}^n$ (random number)

Step3: $C=\langle U, V, W \rangle$

$U=rP$, $U \in \mathbb{G}$;

$V=\sigma \oplus H_2(e(Q_{ID}, X_{ID}+P_{pub})^r)$;

$W=M \oplus H_4(\sigma)$;

C : Ciphertext

4. Decryption phase

Step1: $g_{PKG}=e(d_{ID1}, U)$

Step2: $g_{ID}=e(d_{ID2}, U)$

Step3: $\sigma'=V \oplus H_2(g_{PKG} \cdot g_{ID})$

$M'=W \oplus H_4(\sigma')$

$r'=H_3(\sigma', M')$

Valid → if $r'=r$,then $M=M'$; else failure;

M: Plaintext

Fig. 5.3. PKG-Node IBE algorithm diagram.

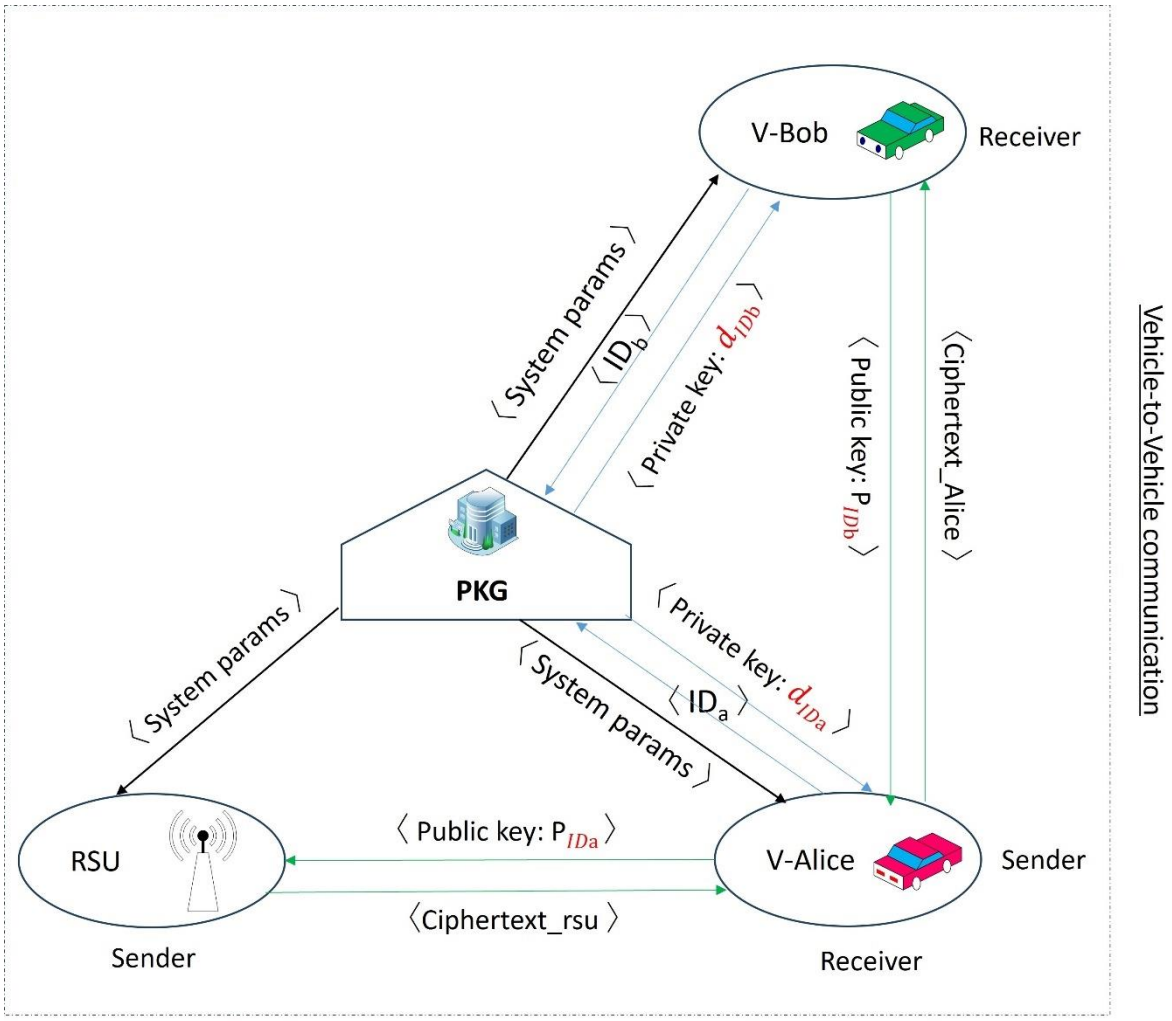

Fig. 5.4. The communication scenario by P-N-IBE in CCN vehicular network.

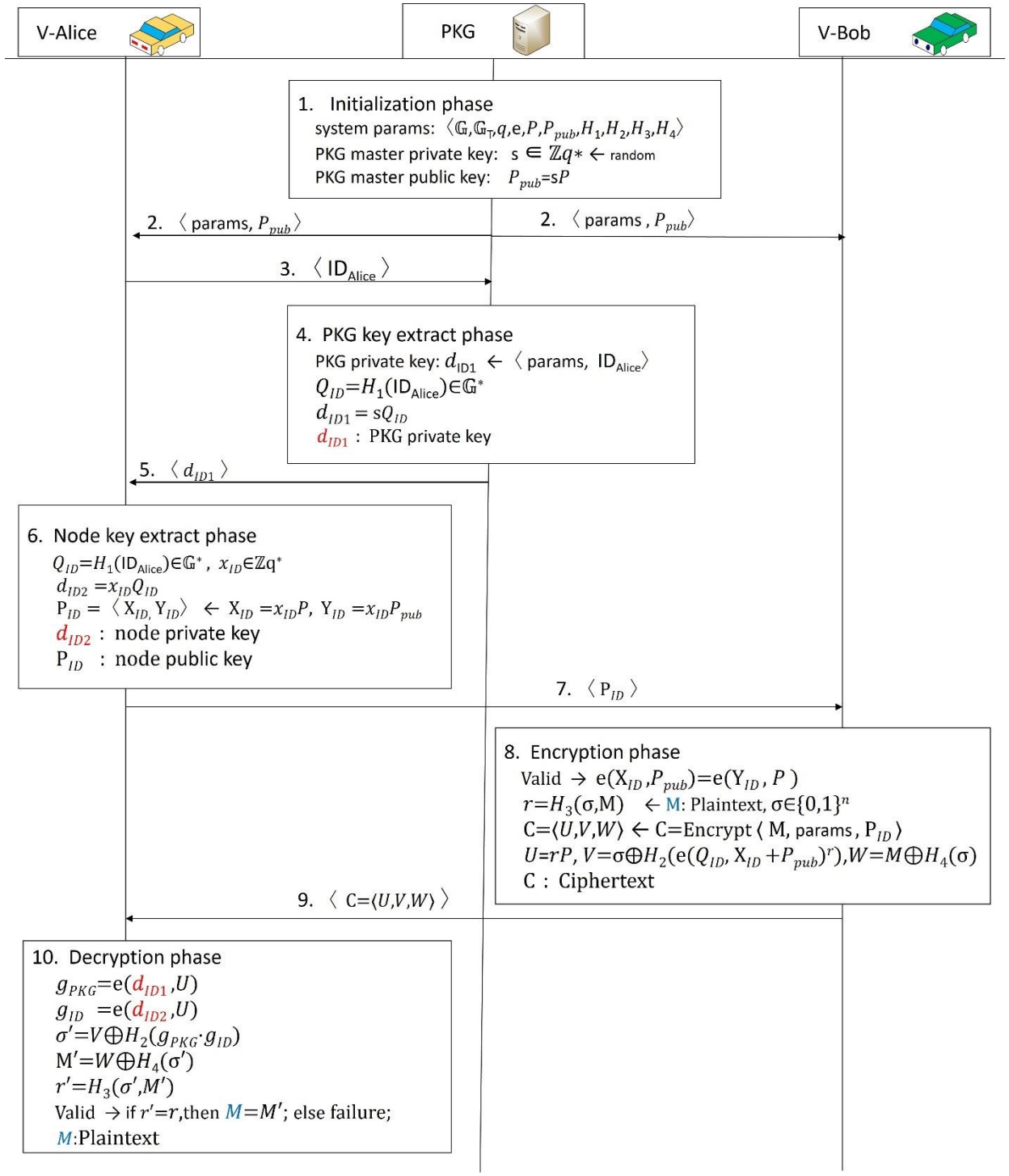

Fig. 5.5. The sequence diagram of P-N-IBE scheme for CCN vehicular network.

Chapter 6

Conclusion and Future work

This dissertation has explored the challenges, opportunities and securities in enhancing content distribution within vehicular networks by CCN paradigms. We proposed a CCN-based scheme that adds CCN framework into DSRC standard for facilitating content propagation in vehicular networks and demonstrate the feasibility that a CCN framework might be working on the top of DSRC standard relying on modifying beacon and WSA message acting as Interest and Advertisement message of CCN. Certainly, to leverage CCN paradigm in vehicular networks could result in sophisticated amendment on DSRC standard, that means quantity of IEEE specifications and frames format might be involved in, however, in this research just limit and basic efforts are done. In addition, according to the characteristic of vehicular networks, hierarchical structure of naming, on-path routing, Leave Copy Everywhere of cache strategy, and Least Frequently Used algorithm are leveraged for vehicular CCN paradigm, which demonstrated that CCN paradigms offer a viable and superior alternative to traditional TCP/IP-based solutions for content distribution in vehicular networks. The proposed framework has shown substantial improvements in data delivery ratios, latency reduction, and network scalability, making it well-suited for real-world deployment in diverse vehicular environments. Furthermore, this dissertation presents a comprehensive analysis and solution to the key escrow problem in IBE systems, specifically tailored for CCN based vehicular networks. By addressing both key escrow and key leakage vulnerabilities, this study contributes to the ongoing development of secure vehicular networks.

The proposed strategies and schemes have been thoroughly evaluated through extensive simulations, yielding several findings and insights.

Enhancements in Content Distribution The integration of the Leave Copy Everywhere (LCE) in-network caching strategy has shown substantial improvements in data delivery ratios and network robustness, especially in urban environments characterized by high building density and frequent signal obstructions. By caching content at multiple nodes within the network, LCE ensures that data is readily available closer to the requesting vehicles, thereby reducing latency and increasing the overall efficiency of content dissemination.

Reduction in RSU Dependency One of the key contributions of this research is the significant reduction in reliance on Roadside Units (RSUs) for content distribution. Traditional TCP/IP-based solutions heavily depend on RSUs for data relay, which incurs high infrastructure costs and maintenance challenges. The proposed CCN-based strategies, particularly the hierarchical naming and on-path routing mechanisms, enable more

autonomous Vehicle-to-Vehicle communication, minimizing the need for constant RSU (road-side-unit) support. This shift not only reduces costs but also enhances network resilience and scalability.

Scalability and Reliability We construct an effective simulation platform for credibility validation in realistic deployment. Proposed large-scale simulation platform represents a major leap forward in the field of vehicular network research. Based this platform, various traffic loads and mobility patterns are simulated. performance metrics demonstrate high scalability and reliability, which provide robust evidence of the framework's capability to handle different network conditions.

Initial solution exploration for key escrow problem and key leakage vulnerabilities A solution of PKG-Node distributed encryption algorithm effectively distributes the key generation process between the PKG and individual vehicle nodes, thereby reducing the risk of a single point of failure and enhancing overall network security. Additionally, the algorithm introduces a timeliness strategy for public keys based on vehicle identity IDs, assigning expiration dates to mitigate key leakage risks. This ensures that compromised keys have limited utility, further strengthening the security framework.

While the research presented in this dissertation provides an initial foundation for enhancing content distribution in vehicular networks, several avenues for future work remain:

Further Optimization of Caching Algorithms Future research can explore the optimization of caching algorithms beyond LCE and LRU. Techniques such as machine learning-based predictive caching and adaptive caching strategies could be investigated to further enhance content availability and reduce latency.

Integration with Emerging Technologies The integration of the proposed framework with emerging technologies such as 5G and edge computing presents a promising direction. 5G's high bandwidth and low latency capabilities, combined with edge computing's proximity to data sources, can complement the proposed CCN strategies, leading to even more efficient content distribution.

Real-World Deployment and Testing While extensive simulations have validated the proposed framework, real-world deployment and testing are crucial for assessing its performance in live vehicular environments. Field trials in urban areas can provide valuable insights into the practical challenges and benefits of the proposed strategies.

Security and Privacy Considerations As vehicular networks handle sensitive data, ensuring security and privacy is paramount. Future research can focus on developing robust security mechanisms to protect data integrity and user privacy within the CCN framework.

Extending Support for New Applications The scope of applications supported by the proposed framework can be extended to include emerging vehicular services such as autonomous driving, smart traffic management, and Vehicle-to-Everything (V2X) communication. These applications have unique requirements that can benefit from the enhanced content distribution capabilities of the proposed strategies.

By addressing these future research directions, the proposed CCN-based in-network caching framework can continue to evolve, contributing to the advancement of vehicular communication systems and the realization of more efficient, reliable, and user-centric transportation networks.

References

[1] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher and B. Ohlman, "A survey of information-centric networking," IEEE Communications Magazine, vol. 50 (7), pp. 26-36, July 2012.

[2] J. Choi, J. Han, E. Cho, et al. "A survey on content-oriented networking for efficient content delivery," IEEE Communications Magazine, vol. 49 (3), pp. 121-127, 2011.

[3] V. Jacobson et al., "Networking Named Content," CoNEXT '09, New York, NY, pp. 1-12, 200.

[4] I. Psaras, WK. Chai and G. Paviou, "In-network cache management and resource allocation for information-centric networks," IEEE Transactions on Parallel and Distributed Systems, vol. 25 (11), pp. 2920- 2930, November 2014.

[5] F. Bai and B. Krishnamachari, "Exploiting the wisdom of the crowd: localized, distributted information centric VANETs," IEEE Communication Magazine, Vol. 48 (5), pp. 138-146, May 2010.

[6] M. Sathiamoorthy, A. G. Dimakis, B. Krishnamachari and F. Bai,"Distributed Storage Codes Reduce Latency in Vehicular Networks," IEEE Trans. on Mobile Computing, vol. 13 (9), pp. 2016–2027, September 2014.

[7] L. Zhang, R. Wakikawa, R. Kunzi, R. Vuyyuru, and L. Zhang, "Data Naming in Vehicle-to-Vehicle Communications," IEEE INFOCOM 2012 Workshop on Emerging Design Choice in Name-Oriented Networking Workshop, USA, pp. 328-333, March 2012.

[8] F. Malandrino, C. Casetti, C.F. Chiasserini and M. Fiore, "Optimal Content Downloading in Vehicular networks," IEEE Transaction on Mobile Computing, vol. 12 (7), pp. 1377-1391, July 2013.

[9] Z. Li, G. Simon, "Time-Shifted TV in content centric networks: The case for cooperative in-network caching," Proc. of the 2011 IEEE Int'l Conf. on Communications (ICC). pp. 1-6, 2011.

[10] The Cisco Visual Networking (VNI) Forecast 2009-2014, Cisco, June 2010 "The New General Service List." http://www.newgeneralservicelist.org, Accessed on 2019.

[11] M. Amadeo, C. Campolo, and A. Molinaro, "CCVN: A Paradigm Shift towards Content-Centric Networking in VANETs" RIUNIONE ANNUALE 2012, pp. 25-27, Giugno, 2012.

[12] J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," Proc. of the IEEE, vol.99 (7), pp. 1162- 1182, July 2011.

[13] http://veins.car2x.org/.

[14] C. Sommer, D. Eckhoff and F. Dressler, "IVC in Cities: Signal Attenuation by Buildings and How Parked Cars Can Improve the Situation," IEEE Transactions on Mobile Computing, vol. 13 (8), pp. 1733-1745, August 2014.

[15] C. Sommer, D. Eckhoff, R. German and F. Dressler, "A Computationally Inexpensive Empirical Model of IEEE 802.11p Radio Shadowing in Urban Environments," Proc. of 8th IEEE/IFIP Conference on Wireless On demand Network Systems and Services, pp. 84-90, Italy, January 2011.

[16] I. Psaras, WK. Chai, G. Pavlou, "Probabilistic in-network caching for information-centric networks," Proc. of the 2nd ICNWorkshop on Information-Centric Networking, pp. 55-60, 2012.

[17] N. Laoutaris, H. Che, I. Stavrakakis, "The LCD interconnection of LRU caches and its analysis," Performance Evaluation, vol. 63 (7), pp. 609- 634, 2006.

[18] K. Cho, M. Lee, K. Park, TT. Kwon, Y. Choi, S. Pack, "WAVE: Popularity-Based and collaborative in-network caching for contentoriented networks," Proc. of the IEEE INFOCOM Workshop on NOMEN, 2012.

[19] S. Wang, J. Bi, JP. Wu, "Collaborative caching based on hash-routing for information-centric networking," Proc. of the ACM SIGCOMM, pp. 535-536, 2013.

[20] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," IEEE Communications Magazine, vol.50, no.7, pp.26–36,2012.

[21] J. Choi, J. Han, E. Cho, T. T. Kwon, and Y. Choi, "A survey on content-oriented networking for efficient content delivery," IEEE Communications Magazine, vol.49, no.3, pp.121–127,201.

[22] V.Jacobson,D.K.Smetters,J.D.Thornton,M.F.Plass,N. H. Briggs, and R. L. Braynard, "Networking named content," in Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies (CoNEXT'09),pp.1–12,ACM,Rome,Italy,2009.

[23] I. Psaras, W. K. Chai, and G. Pavlou, "In-network cache management and resource allocation for information-centric networks," IEEE Transactions on Parallel and Distributed Sys-tems, vol.25, no.11, pp.2920–2931,2014.

[24] F. Bai and B. Krishnamachari, "Exploiting the wisdom of the crowd: localized, distributed information-centric VANETs," IEEE Communications Magazine, vol. 48, no. 5, pp. 138–146, 2010.

[25] M.Sathiamoorthy, A.G.Dimakis, B.Krishnamachari, and F. Bai, "Distributed storage codes reduce latency in vehicular networks," IEEE Transactions on Mobile Computing,vol.13,no. 9, pp. 2016–2027, 2014.

[26] L.Wang, R.Wakikawa, R.Kuntz, R.Vuyyuru, and L.Zhang, "Data naming in vehicle-to-vehicle communications," in Proceedings of the IEEE Workshop on Emerging Design Choice in Name-Oriented Networking Workshop (INFOCOM '12),pp. 328–333,Orlando,Fla,USA,March201.

[27] F. Malandrino, C. Casetti, C.F. Chiasserini, and M. Fiore, "Optimal content downloading in vehicular networks," IEEE Transactions on Mobile Computing, vol.12, no.7, pp.1377–1391, 2013.

[28] Z. Li and G. Simon, "Time-shifted TV in content centric networks: the case for cooperative in-network caching," in Proceedings of the IEEE International Conference on Communi- cations (ICC '11), pp. 1–6, Kyoto, Jap an, June 2 011.

[29] Cisco, the Cisco Visual Networking (VNI) Forecast 2009–2014, Cisco, 2010.

[30] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," Proceedings of the IEEE, vol.99, no. 7, pp. 1162–1182, 2011.

[31] M. Amadeo, C. Campolo, and A. Molinaro, "Content-centric networking: is that a solution for upcoming vehicular networks," in Proceeding of the 9th ACM International

Workshop on Vehicular Inter-Networking, Systems, and Applications (VANET '12), pp.99-102, Ambleside, UK, June2012.
[32] "Reducing Environmental Footprint based on Multi-Modal Fleet management Systems for Eco-Routing and Driver Behaviour Adaptation (REDUCE)," 2014, http://cordis.europa.eu/ docs/projects/cnect/4/288254/080/deliverables/003-D631.pdf.
[33] https://w w w.openstreetmap.org/.
[34] https://omnetpp.org/.
[35] http://veins.car2x.org/.
[36] http://sumo.dlr.de/wiki/Main Page.
[37] C. Sommer, D. Eckhoff,and FDressler,"IVC incities: signal attenuation by buildings and how parked cars can improve the situation," IEEE Transactions on Mobile Computing,vol.13,no. 8, pp. 1733–1745, 2014.
[38] C. Sommer, D. Eckhoff, R. German, and F. Dressler, "A computationally inexpensive empirical model of IEEE 802.11p radio shadowing in urban environments," in Proceedings of the 8th IEEE/IFIP Conference on Wireless On-Demand Network Systems and Services (WONS '11), pp. 84–90, Bardonecchia, Italy, January 2014.
H. Cheng, X. Fei, A. Boukerche, and M. Almulla, "GeoCover: an efficient sparse coverage protocol for RSU deployment over urban VANETs," Ad Hoc Networks, vol.24, pp.85–102, 2011.
[39] H. Cheng, X. Fei, A. Boukerche, and M. Almulla, "GeoCover: an efficient sparse coverage protocol for RSU deployment over urban VANETs," Ad Hoc Networks, vol.24, pp.85–102,2015.
[40] Q. Chen, D. Jiang, and L. Delgrossi, "IEEE 1609.4 DSRC multi- channel operations and its implications on vehicle safety communications," in Proceedings of the IEEE Vehicular Networking Conference (VNC '09), pp. 1–8, October 2009.
[41] F. Malandrino, C. Casetti, F. Chiasserini, C. Sommer, and F. Dressler, "The role of parked cars in content downloading for vehicular networks," IEEE Transactions on Vehicular Technology, vol.63, no.9, pp.4606–4617, 2014.
[42] I.Psaras, W.K.Chai,andG.Pavlou,"Probabilisticin-network caching for information-centric networks," in Proceedings of the 2nd ICN Workshop on Information-Centric Networking,pp.55– 60, 2012.
[43] N. Laoutaris, H. Che, and I. Stavrakakis, "The LCD interconnection of LRU caches and its analysis," Performance Evaluation, vol.63, no.7, pp. 609–634, 2006.
[44] K. Cho, M. Lee, K. Park, T. T. Kwon, Y. Choi, and S. Pack, "WAVE: popularity-based and collaborative in-network caching for content-oriented networks," in Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS '12), pp. 316–321, Orlando, Fla, USA, March 2012.
[45] S. Wang, J. Bi, and J. Wu, "Collaborative caching based on hash- routing for information-centric networking," in Proceedings of the ACM SIGCOMM 2013 conference on Information-Centric Networking (SIGCOMM '13), pp. 535–536, ACM, Hong Kong, 2013.
[46] J. Guo and N. Balon, "Vehicular Ad Hoc Networks and Dedicated Short-Range Communication, "http://nbalon.info/projects/cis695/vanet chapter.pdf, June 2006.
[47] Y. Li, "An Overview of the DSRC/WAVE Technology," Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol.74, pp.544–558, 2011.
[48] F. Malandrino, C. Casetti, C.F. Chiasserini, C. Sommer, and F. Dressler, "The Role of

Parked Cars in Content Downloading for Vehicular Networks," IEEE Trans. Veh. Technol., vol.63, no.9, pp.4606–4617, Nov. 2014, doi: 10.1109/TVT.2014.2316645.
[49] C. Makaya and S. Pierre, Emerging Wireless Networks, CRC press, 2011.
[50] Z. Wang and M. Hassan, "How Much of DSRC is Available for Non-Safety Use?," Proc. fifth ACM International Workshop on Mobile Computing and Networking, pp.23–29, Sept. 2008, doi: 10.1145/1410043.1410049.
[51] D.S. Coming and O.G. Staadt, "Velocity-Aligned Discrete Oriented Polytopes for Dynamic Collision Detection," IEEE Trans. Vis. Comput. Graphics, vol.14, no.1, pp.1–12, Feb. 2008, doi: 10.1109/TVCG.2007.7040.
[52] F. Bai and B. Krishnamachari, "Exploiting the Wisdom of the Crowd: Localized, Distributed Information-Centric VANETs," IEEE Commun. Mag., vol.48, no.5, pp.138–146, May 2010, doi: 10.1109/MCOM.2010.5458375.
[53] V. Jacobson, D.K. Smetters, J.D. Thornton, M.F. Plass, N.H. Briggs, and R.L. Braynard, "Networking Named Content," Proc. 5th international conference on Emerging networking experiments and technologies (CoNEXT '09), pp.1–12, Dec. 2009, doi: 10.1145/1658939.165894.
[54] G. Xylomenos, C.N.Ververidis, V.A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K.V. Katsaros, and G.C. Polyzos, "A Sur- vey of Information-Centric Networking Research," IEEE Communications Surveys & Tutorials, vol.16, no.2, pp.1024–1049, July 2014, doi: 10.1109/SURV.2013.070813.00063.
[55] J. Choi, J. Han, E. Cho, T. Kwon, and Y. Choi, "A Survey on Content-Oriented Networking for Efficient Content Delivery," IEEE Commun. Mag., vol.49, no.3, pp.121–127, March 2011, doi: 10.1109/MCOM.2011.5723809.
[56] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A Survey of Information-Centric Networking," IEEE Commun. Mag., vol.50, no.7, pp.26–36, July 2012, doi: 10.1109/ MCOM.2012.6231276.
[57] J.B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," Proc. IEEE, vol.99, no.7, pp.1162–1182, July 2011, doi: 10.1109/JPROC.2011.2132790.
[58] S.A.M. Ahmed, S.H.S. Ariffn, and N. Fisal, "Overview of Wire- less Access in Vehicular Environment (WAVE) Protocols and Standards," Indian Journal of Science and Technology, vol.6, no.7, July 2013, doi: 10.17485/ijst/2013/v6i7/34355.
[59] Q. Chen, D. Jiang, and L. Delgrossi, "IEEE 1609.4 DSRC Multi-Channel Operations and Its Implications on Vehicle Safety Communications," Proc. IEEE Vehicular Networking Conference (VNC), pp.1–8, Oct. 2009, doi: 10.1109/VNC.2009.541639.
[60] F. Malandrino, C. Casetti, C.F. Chiasserini, and M. Fiore, "Optimal Content Downloading in Vehicular networks," IEEE Trans. Mobile Comput., vol.12, no.7, pp.1377–1391, July 2013, doi: 10.1109/TMC.2012.115.
[61] H. Tian, Y. Otsuka, M. Mohri, Y. Shiraishi and M. Morii, "LCE In-Network Caching on Vehicular Networks for Content Distribu- tion in Urban Environments," Proc. seventh International Confer- ence on Ubiquitous and Future Networks (ICUFN'15), pp.551–556, July 2015, doi: 10.1109/ICUFN.2015.7182605.
[62] C. Campolo, H.A. Cozzetti, A. Molinaro, and R. Scopigno, "Augmenting Vehicle-to-Roadside Connectivity in Multi-channel Vehicular Ad Hoc Networks," Journal of Network and Computer Applications, vol.36, no.5, pp.1275–1286, Sept. 2013, doi: 10.1016/j.jnca.2012.04.001.
[63] B.T. Sharef, R.A. Alsaqour, and M. Ismail, "Vehicular Communication Ad Hoc Routing Protocols: A survey," Journal of Network and Computer Applications, vol.40, pp.363–

396, April 2014, doi: 10.1016/j.jnca.2013.09.008.

[64] C. Sommer, D. Eckhoff, and F. Dressler, "IVC in Cities: Signal Attenuation by Buildings and How Parked Cars Can Improve the Situation," IEEE Trans. Mobile Comput., vol.13, no.8, pp.1733–1745, Aug. 2014, doi: 10.1109/TMC.2013.80.

[65] C. Sommer, D. Eckhoff, R. German, and F. Dressler, "A Computationally Inexpensive Empirical Model of IEEE 802.11p Radio Shad- owing in Urban Environments," Proc. Eighth International Conference on Wireless On-Demand Network Systems and Services (WONS), pp.84–90, Jan. 2011, doi: 10.1109/WONS.2011.5720204.

[66] F. Bai and B. Krishnamachari, "Spatio-Temporal Variations of Vehicle Traffic in VANETs: Facts and Implications," Proc. 6th ACM International Workshop on Vehicular InterNETworking (VANET'09), pp.43–52, Sept. 2009, doi: 10.1145/1614269.1614278

[67] I.C. Msadaa, P. Cataldi, and F. Filali, "A Comparative Study be- tween 802.11p and Mobile WiMAX-Based V2I Communication Networks," Proc. Fourth International Conference on Next Generation Mobile Applications, Services and Technologies, pp.186–191, July 2010, doi: 10.1109/NGMAST.2010.45

[68] L. Wang, R. Wakikawa, R. Kuntz, R. Vuyyuru, and L. Zhang, "Data Naming in Vehicle-to-Vehicle Communications," IEEE Conference on Computer Communications Workshop (INFOCOM WKSHPS'12), pp.328–333, March 2012, doi: 10.1109/ INFCOMW.2012.6193515

[69] M. Amadeo, C. Campolo, and A. Molinaro, "Content-Centric Networking: is that a Solution for Upcoming Vehicular Networks," Proc. ninth ACM international workshop on Vehicular inter-net- working, systems, and applications, pp.99–102, June 2012, doi: 10.1145/2307888.2307906

[70] F. Malandrino, C. Casetti, C.-F. Chiasserini, C. Sommer, and F. Dressler, "The Role of Parked Cars in Content Downloading for Vehicular Networks," IEEE Trans. Veh. Technol., vol.63, no.9, pp.4606–4617, Nov. 2014, doi: 10.1109/TVT.2014.2316645.

[71] H. Cheng, X. Fei, A. Boukerche, and M. Almulla, "GeoCover: An Efficient Sparse Coverage Protocol for RSU Deployment over Urban VANETs," Ad Hoc Networks, vol.24, Part B, pp.85–102, Jan. 2015, doi: 10.1016/j.adhoc.2014.07.022

[72] Z. Yan, S. Zeadally, and Y.-J. Park, "A Novel Vehicular Infor- mation Network Architecture Based on Named Data Networking (NDN)," IEEE IoT Journal, vol.1, no.6, pp.525–532, Dec. 2014, doi: 10.1109/JIOT.2014.2354294

[73] C.D. Castro, C. Raffaelli, and O. Andrisano, "A Dynamic Hier- archical VANET Architecture for Named Data Networking Ap- plications," Proc. 2015 IEEE Int. Conf. on Communications, pp.3659–3665, June 2015, doi: 10.1109/ICC.2015.7248893

[74] https://en.wikipedia.org/wiki/Contentcentric networking

[75] A. Ioannou and S. Weber, "Towards On-path Caching Alternatives in Information-Centric Networks," Proc. IEEE 39th Conf. on Local Computer Networks (LCN), pp.362–365, Sept. 2014, doi: 10.1109/LCN.2014.692579.

[76] M. Draxler and H. Karl, "Efficiency of On-Path and Off-Path Caching Strategies in Information Centric Networks," Proc. IEEE International Conference on Green Computing and Communications, pp.581–587, Nov. 2012. doi: 10.1109/GreenCom.2012.82.

[77] LAN/MAN Standards Committee in IEEE Computer Society, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 2012.

[78] I. Psaras, W.K. Chai, and G. Pavlou, "Probabilistic In-Network Caching for

Information-Centric Networks," Proc. second Edition of the ICN Workshop on Information-Centric Networking, pp.55–60, Aug. 2012, doi: 10.1145/2342488.2342501.

[79] N. Laoutaris, H. Che, and I. Stavrakakis, "The LCD interconnection of LRU Caches and Its Analysis," Performance Evaluation, vol.63, no.7, pp.609–634, July 2006, doi: 10.1016/j.peva.2005.05.003.

[80] K. Cho, M. Lee, K. Park,T.T. Kwon, Y. Choi,and S. Pack, "WAVE: Popularity-Based and Collaborative In-Network Caching for Contentoriented Networks," Proc. IEEE INFOCOM Workshop on NOMEN, pp.25–30, March 2012, doi: 10.1109/INFCOMW. 2012.6193512.

[81] S. Wang, J. Bi, and J. Wu, "Collaborative caching based on hash-routing for information-centric networking," Proc. ACM Conference on SIGCOMM (SIGCOMM '13), pp.535–536, Oct. 2013, doi: 10.1145/2486001.2491727.

[82] Z. Li and G. Simon, "Time-Shifted TV in Content Centric Net- works: The case for Cooperative In-Network Caching," Proc. IEEE Int'l Conf. on Communications (ICC), pp.1–6, June 2011, doi: 10.1109/icc.2011.5963380.

[83] https://www.openstreetmap.org/.

[84] https://omnetpp.org/.

[85] http://veins.car2x.org/.

[86] http://sumo.dlr.de/wiki/Main Page.

[87] P. Salvo, F. Cuomo, A. Baiocchi, and A. Bragagnini, "Road Side Unit Coverage Extension for Data Dissemination in VANETs," Proc. ninth Ann. Conf. on Wireless On-demand Network Systems and Ser- vices (WONS), pp.47–50, Jan. 2012, doi: 10.1109/WONS.2012. 6152235.

[88] B. Ginzburg and A. Kesselman, "Performance Analysis of A-MPDU and AMSDU Aggregation in IEEE 802.11n," Proc. IEEE Sarnoff Symposium, pp.1–5, May 2007, doi: 10.1109/SARNOF.2007. 4567389.

[89] G. Pavlou, "Information-Centric Networking and In-Network Cache Management," IFIP/IEEE CNSM 2013 Keynote Speech, http://www.ee.ucl.ac.uk/~gpavlou/, Oct. 2013.

[90] S. Arianfar, P. Nikander, and J. Ott, "On Content-Centric Router De- sign and Implications," Proc. ACM ReArch the Internet Workshop, Nov. 2010. doi: 10.1145/1921233.1921240.

[91] D. Perino and M. Varvello, "A Reality Check for Content Centric Networking," Proc. ACM SIGCOMM Workshop on Information- Centric Networking (ICN '11), pp.44–49, Aug. 2011, doi: 10.1145/ 2018584.2018596.

[92] C. Adams and S. L, "Understanding PKI: Concepts, Standards, and Deployment Considerations," 2003, ISBN: 978-0-672-32391-1.

[93] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal on Computing, Vol. 32, No. 3, pp. 213-229, 2001, doi: 10.1007/ 3-540-44647-8_13.

[94] Gentry, Craig, "Certificate-based encryption and the certificate revocation problem," Proc. Of the 22nd international conference on Theory and applications of cryptographic techniques, pp. 272-293, 2003, doi: 10.1007/3-540-39200-9_17.

[95] S. Sattam and G. Kenneth, "Certification Public Key Cryptograph," 9th International Conference on the theory and Application of Cryptology and information Security, pp. 213-229, 2003, doi: 10.1007/978-3-540-40061-5_29.

[96] M. Patel and R. Patel, "Improved identity based encryption system (Iibes): A mechanism for eliminating the key-escrow problem," Emerging Science Journal, Vol. 5, No. 1, pp. 1-10, 2021, doi: 10.28991/esj-2021-01256.

[97] Q. Wei, F. Qi and Z. Tang, "Remove key escrow from the BF and Gentry identity-based encryption with non-interactive key generation," Telecommunication Systems, Vol. 68, No. 1, pp. 27-39, 2018, doi: 10.1007/s11235-018-0474-5.

[98] R. Gennaro, and S. Jarecki, "Secure Distributed Key Generation for Discrete-Log Based Cryptosystems," Journal of Cryptology, Vol. 20, No. 1, pp. 51-83, 1999, doi: 10.1007/s00145-006-0347-3.

[99] H. Chen, S. Zhang and Q. Li "Distributed Key Generation for Secure Multi-party Computation," ACM Transactions on Privacy and Security, Vol. 24, No. 1, pp. 1-29, 2020, doi: 10.1145/3441437.

[100] J. Wang and Q. Cheng, "Secure and Efficient Distributed Key Generation for IoT Devices," IEEE Transactions on Industrial Informatics, Vol. 17, No. 6, pp. 4132-4142, 2021, doi: 10.1109/TII.2020.3032435.

[101] S. S. Al-Riyami and K. G.Paterson, "Certificateless public key cryptography," In Advances in Cryptology, Vol. 2894, pp. 452-473, 2003, doi: 10.1007/978-3-540-40061-5_29.

[102] W. Tang, "Research on IBE Algorithm and Application in Internet of Things," Thesis of Nanjing University of Post for master's degree, pp. 26-33, 2020.

[103] P. W. Shor "Algorithms for quantum computation: discrete logarithms and factoring," In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 124-134, 1994, doi: 10.1109/SFCS.1994.365700.

[104] A. Boldyreva, M. Fischlin and A. Palacio "A closer look at PKI: Security and efficiency," In Cryptography and Theory in Public-Key Infrastructure, Springer, pp. 73-89, 2007, doi: 10.1007/978-3-540-77339-6_6.

[105] H. D. Phaneendra, "Identity-based cryptography and comparison with traditional public key encryption: A survey," International Journal of Computer Science and Information Security, Vol. 12, No. 2, pp. 15-22, 2014, doi: 10.5121/ijcsa.2014.120203.

[106] D. Mahto, and D. Yadav,"RSA and ECC: A comparative analysis," International Journal of Applied Engineering Research, Vol. 12, No. 19, pp. 8925-8932, 2017, doi: 10.1007/s10207-017-0379-8.

[107] N. Garg, and P. Yadav,"Comparison of asymmetric algorithms in cryptography," Journal of Computer Science and Mobile Computing, Vol. 3, No. 4, pp. 741-747, 2014, doi: 10.1007/s10207-014-0226-3.

[108] M. Sato, M. Mohri, H. Doi and Y. Shiraishi, "Partially Doubly-Encrypted Identity-Based Encryption Constructed from a Certain Scheme for Content Centric Networking," Journal of Information Processing, Vol. 24, No. 1, pp. 2-8, 2016, doi: 10.2197/ipsjjip.24.2.

[109] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," IEEE Symposium on Security and Privacy, Vol. 24, No. 1, pp. 321-334, 2007, doi: 10.1109/SP.2007.11.

[110] D. He, C. Chen, S. Chan, and J. Bu "Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions," IEEE Transactions on Wireless Communications , Vol. 11, No. 1, pp. 48-53, 2011, doi: 10.1109/TWC.2011.110811.111240

Doctoral Dissertation, Kobe University
"Study on Enhancing Content Distribution in Vehicular Network", 79 pages
Submitted on July 10, 2024
When published on the Kobe University institutional repository /Kernel/, the publication date shall appear on the cover of the repository version.