Wide Transmission of Proxy Cooperative Awareness Messages

Masahiro Kitazawa, Manabu Tsukada, Hideya Ochiai, Hiroshi Esaki

▶ **To cite this version:**

Masahiro Kitazawa, Manabu Tsukada, Hideya Ochiai, Hiroshi Esaki. Wide Transmission of Proxy Cooperative Awareness Messages. The Seventh International Conference on Advances in Vehicular Systems, Technologies and Applications (VEHICULAR 2018), Jun 2018, Venice, Italy. hal-01879100

HAL Id: hal-01879100

https://hal.archives-ouvertes.fr/hal-01879100

Submitted on 22 Sep 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Wide Transmission of Proxy Cooperative Awareness Messages

Masahiro Kitazawa, Manabu Tsukada, Hideya Ochiai and Hiroshi Esaki
Graduate School of Information Science and Technology
University of Tokyo, Japan
Email: {ktzw, tsukada, jo2lxq}@hongo.wide.ad.jp, hiroshi@wide.ad.jp

***Abstract*—Recently, autonomous vehicles have become a reality. Most of the research related to autonomous vehicles focuses on the sensors attached to vehicles. However, owing to blind spots, sensors are insufficient for avoiding accidents. Cooperative Intelligent Transport Systems (CITSs) have been introduced to reduce blind spots. These systems wirelessly communicate with other CITS-enabled vehicles and collect road and traffic information. There are two types of messages used in CITS: Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs). CAMs are used to notify the existence of sender. Some issues are known to exist with these messages. Several methods have been proposed to help overcome these issues. One of these methods is Proxy CAM. In this study, we will describe four problems of Proxy CAM and propose Grid Proxy CAM, which builds a network of Proxy CAM devices and forwards Proxy CAM packets. We have been developing two methods for this system. The first is "SDN routing", which uses Software Defined Network (SDN) for route control. The second is "Passive selection", which is used to select incoming Proxy CAM packets. Furthermore, we will discuss the advantages and disadvantages of these methods and the future plan of this ongoing work.**

Keywords–CITS; Proxy CAM; Wide transmission; Grid Proxy CAM; SDN.

I. INTRODUCTION

Interest in autonomous driving has increased recently. Autonomous driving can be divided into several categories, according to function, from Level 0 to Level 5.

- Level 0 (No Automation): the vehicle is unassisted by Artificial Intelligence (AI). Autonomous driving is unavailable.
- Level 1 (Driver Assistance): AI performs only one driving operation, such as steering, acceleration, or deceleration. Automatic braking and adaptive cruise control are examples.
- Level 2 (Partial Automation): AI can do several driving operations simultaneously. Drivers must keep control and monitor the AI's decisions. In Japan, a system called "Pro Pilot" [1] by Nissan accelerates, decelerates, and steers to maintain the inter-vehicular distance and keep to the center of the road by detecting the vehicle in front and road lines.
- Level 3 (Conditional Automation): AI performs every operation of driving. However, if there is an emergency, the AI notifies the driver who takes over. Additionally, there are limitations to the driving environment, such as only highways.
- Level 4 (High Automation): AI does every operation of driving, even during an emergency. However, there is a limitation of the environment.
- Level 5 (Full Automation): AI does every operation in all circumstances. The driver does not need to keep watch. All passengers are free from driving.

For now, Levels 1 and 2 are commercialized, and Levels 3 and 4 are realized only at the research level. Intelligent Transport Systems (ITSs) manage problems related to an accident, traffic jam, environmental pollution, and the pursuit of convenience and comfort in road traffic. Autonomous driving is a key ITS technology, and the main research field is now stand-alone.

ITSs use only the vehicle's own sensors to make the next move. However, at an intersection, there is always a blind spot (i.e., an area the sensors cannot detect), and this often contributes to accidents. Cooperative ITS (CITS) [2] is a system that utilizes the communication among vehicles and roadside units (RSU) to share road traffic information and make blind spots smaller. Additionally, because this system can get the information from a distance, vehicles can change paths to avoid traffic jams, thus increasing convenience.

There are problems with designing the CITS network among vehicles and RSUs because of the communications protocols and the wireless technologies needed to create a real-time control system. Vehicles move very fast. Thus, vehicle information has a very short life span. This causes each vehicle to broadcast the information at a high frequency. The delay between sending and receiving also must be very short. The active distribution and balancing of network traffic is also very important. IEEE 802.11p [3] is a wireless technology for connecting vehicles, but it has a low fault tolerance and a short range, which must be improved for CITS.

In this work, we propose Grid Proxy Cooperative Awareness Message, to solve the problem of dispersing network traffic load and to improve the low fault tolerance and short range of IEEE 802.11p. There are two methods to realize this system: Software Defined Network (SDN) routing and passive selection. We describe these methods and discuss their advantages and disadvantages in this paper. By leveraging our previous work, Remote Proxy CAM [4], we improve the safety of Grid Proxy CAM.

The rest of this paper is organized as follows. Section II highlights CITS in detail, including protocol stack and two types of messages. Section III discusses related works, such as SDN, routing control, and Vehicular Ad-hoc Network (VANET). Additionally, we introduce works that have attempted to solve SDN's problems. In Section IV, we describe IEEE 802.11p's problems of network traffic load, low fault tolerance, and short range. In Section V, we finally define Grid Proxy CAM to solve the problems. Section VI concludes our paper and presents our future studies.

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-643-9

II. CITS

CITS is being designed to make road traffic more convenient and safer. The stand-alone system uses only the information from the sensors attached to vehicles to assist the driver's operation. However, CITS also enables vehicles to communicate with vehicles and RSUs and share information about road traffic. With this combined information, CITS-enabled vehicles can serve as better driving assistants and make better decisions. There are CITS architectures designed separately in Europe, America, and Japan. In this work, we focus on European CITS architecture.

CITS is composed of four primary layers: application, facility, network & transport, and access. There is also a management layer that manages the facility, network & transport, and access layers and a security layer that is responsible for CITS safety.

The access layer manages the wireless technologies (e.g., Long Term Evolution (LTE) and IEEE 802.11p [3]) and the network & transport layer manages the route control (e.g., GeoNetworking [5] and Basic Transport Protocol [6]). The facility layer summarizes and stores the information from sensors and communication messages to make it easier to utilize for applications, such as local dynamic mapping and other services.

There are two types of CITS communication massages: CAMs [7] and decentralized environmental notification messages (DENM) [8]. CAM is a message that every CITS-enabled vehicle and pedestrian cellphone generates. It contains highly dynamic information. With this type of message, CITS devices recognize the senders' location and vector. Because of CAMs' time sensitivity, messages must be generated at a high frequency, such as the recommended 1-to-10 Hz. CAM information may affect a small range (i.e., 100 m), and to mitigate CITS network bandwidth, messages are single-hop broadcasted. Thus, CAM message forwarding is not recommended. However, DENMs are messages that contain relatively static information about events that affect road and traffic conditions, such as construction, accidents, and weather. There is no recommendation for the frequency of transmission. So, CITS devices transmit DENMs according to their own configurations. DENM is recommended to multi-hop because the information it contains is considered to affect a wide range. When a CITS device receives CAMs and DENMs, they are delivered to facility layer and processed to provide the information to the application layer.

III. Related Works

A. SDN

In legacy networks, protocols, such as Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) perform routing control according to certain algorithms. Special route configuration for each node must also be performed manually. However, if there is a replacement of nodes or a change in network topology, the configuration must be also performed manually. They cost a lot to maintain. However, with SDNs, a controller manages network routing. Thus, it does not need to be configured manually. In legacy networks, route control and data transmission is performed on the same network. In SDN, it is done on two separate networks: a control plane and a data plane. The control plane is composed of switches and a server (i.e., controller). This plane is used for sending control messages for routing and switch configuration, and for sending "packet-in" messages to notify the existence of a packet that does not match any routing configuration. The data plane is composed of switches and nodes. This network is used for transmitting and receiving data packets. In this work, we use Open Flow [9], a technology that supports SDN.

In Open Flow, routing configurations are called flow entries and are stored in a flow table. Flow entries are composed of rule and action fields. The rule field includes a condition; the switch checks if an incoming packet satisfies the condition. The action field includes an operation; the switch performs the operation if the packet meets the condition. The rule and action fields can be described by layers 1∼4 of the Open Systems Interface reference model. If the controller modifies switch flow entries, it sends a "Flow-Mod" message to the switch. Then, whenever the switch receives a packet, it checks the flow table and performs the appropriate operation. If no flow entry requirement is met, the switch drops the packet or sends a "Packet-In" message to the controller. Then, the controller responds with "Packet-Out."

B. VANET

The Vehicular Ad-hoc network (VANET) is a system that enables CITS-enabled vehicles to form an ad-hoc network and communicate. All vehicles must perform routing control because of the ad hoc nature. The wireless technology used in VANET is IEEE 802.11p [3]. It is designed to enable fast-moving nodes to communicate, and it uses a high-frequency band (i.e., 5.9 GHz) because the distance between the nodes changes very fast and the time during which nodes remain within the communication range is very short; hence the speed of data communication must be fast.

One of the problems associated with VANETs is the occupancy of the communication bandwidth by periodic packets, such as CAMs. The higher the frequency of CAM transmission, the safer the road traffic becomes. However, increasing the frequency also increases the bandwidth occupancy due to higher data traffic. Hence, in a urban areas where the vehicle density is high, the transmission of CAMs exceeds the communication bandwidth and the packets that are transmitted when certain events occur, such as DENMs cannot be transmitted. Additionally, delay and packet loss can occur to the CAM packets themselves.

Another problem is forwarding the packets that need to be broadcasted and forwarded, such as DENMs. Basically, a node that receives such a packet must forward the packet to all nodes that are connected to the node. However, to applying this operation to all nodes could create forwarding loops and a large number of transmissions over a short duration. These transmissions could occupy the communication bandwidth and cause a long delay in the delivery of other messages. This delay is critical to the messages that require real-time property and this must be avoided.

For the first problem associated with VANETs, [10] concluded that nodes establish more connections than needed, making the transmission burden larger. Thus, they proposed fair-power adjustment for vehicular environments to control the network load of periodic packets (e.g., CAM) by setting an upper limit to network connections (i.e., Max Beaconing Load (MBL)). This forbids the number of connections at

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-643-9

each node from exceeding the MBL. To adjust the number of the connections, they utilized the transmit power of wireless technologies. Their method avoided packet loss and delay. Additionally, if multi-hop packets (e.g., DENM) arrived to the network, they were less likely to not be broadcasted.

In [11], periodic packets constituted large data traffic because of the unnecessarily high frequency of transmission. Thus, the researchers proposed an adaptive beaconing rate to adjust the frequency of the transmission according to the surrounding situation and the node's status. They fed vehicle status (i.e., accident status and likelihood of causing an accident) and percentage of same-directional neighbor vehicles (i.e., density of vehicles moving in the same direction) into a fuzzy inference engine to calculate the precise transmission frequency needed for the situation.

For the second problem, [12] proposed The Last One (TLO) algorithm, which forces only the most appropriate nodes to broadcast packets. The algorithm transmits backwards from the sender, which is useful for mitigating an accident. Using Global Positioning System (GPS) information and the predefined distance of the communication range, each vehicle decides whether it is the Last Vehicle (LV) that received the packets from a sender. If so, it broadcasts the packets. To describe this algorithm in detail, if a node receives multi-hop broadcast packets, it receives the GPS information of the sender from the packets and calculates the geographical distance between the sender and the node. Similarly, the node calculates the geographical distance among the surrounding nodes. These nodes' GPS information is delivered from their CAMs. The communication range is common to all nodes and never changes. Thus, the node checks if there is another node behind the transmitting node within the communication range of the sender. If so, the node does not broadcast the packets for a while. If another node does not broadcast the packets and the node does not receive the packets, it concludes it is the LV and broadcasts the packets. Also, if the node cannot find any node that satisfies the condition, it decides that it is the LV and broadcasts the packets. In [13], the authors attempted to solve this problem by using the cellular network. They divided vehicles into two types: Gateway service Providers (GP), which communicate via IEEE 802.11p and cellular wireless technology; and ordinal vehicles, which communicate only via IEEE 802.11p. The periodic packets are assumed effective in for short range from the origin. Thus, they are broadcasted locally via IEEE 802.11p. Multi-hop packets are assumed to have a wider effect. Thus, when they are received by GPs, they send the packets to the cloud server. The server gets the GPS information of the origin from the packets and identifies the area needing the packets to be disseminated and sends them to GPs in that area. When the GPs receive the packets, they rebroadcast them.

C. VANET using SDN

There are many works to solve the problem of the occupancy of the communication bandwidth by massive packets. Recently, some methods have proposed using SDN for dynamic route control.

In [14], vehicles joined both VANET and cellular network and RSUs opened ad-hoc connection with vehicles. Additionally, the SDN controller was connected to RSUs and cellular base stations. The connection between SDN controller and RSUs and the SDN controller and vehicles belongs to control plane and the connection between RSUs and vehicles and vehicles each other belongs to data plane. RSUs and vehicles send information of connected RSUs and vehicles periodically to the SDN Controller via control plane. The SDN controller alters RSUs and vehicles' flow entries according to this information and when some specific nodes send requests to the SDN controller. Also, since vehicles and the SDN controller are connected via wireless technology, the connection can be lost. In that case, each vehicle has a local SDN agent. This agent performs the routing control using ordinal VANET routing protocols (e.g., Greedy Perimeter Stateless Routing (GPSR), Ad-hoc On-Demand Distance Vector (AODV), Destination-Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR)) when the connection to SDN controller is lost.

In [15], the authors proposed the SDN-based Geographic Routing (SDGR) protocol for route control. The network topology is same as in [14]. This protocol is designed to be used when a vehicle sends messages to another vehicle. First, the sender only knows the IP address of the target, but does not know its geographical position. Thus, the sender sends a request to the SDN controller. When the SDN controller receives the request, it uses an optimal forwarding path algorithm. First, the controller identifies the geographical position of the target by using the information from periodic RSUs and vehicles messages sent to the controller. After that, the controller chooses the geographical path that goes through the relatively high density of vehicles in order to not lose the packets and to obtain the shortest path. After choosing the path, the controller replies with the path choice called optimal forwarding path (ofp) to the sender. When the sender receives the ofp, it inserts it into the packets. Using the packet forwarding algorithm and the ofp, the sender selects the next node and transmits the packets. The next node checks the ofp in the packets and uses packet forwarding algorithm to transmit the packets. All nodes in the path do the same operation, and eventually the packets reach the target. In SDGR, there are two modes: forthright mode and junction mode. The forthright mode is used when a vehicle is not at an intersection. When a vehicle is in this mode, it only checks the ofp of the packets and forwards them to the node which is on the path of the ofp, nearest to the target, and connected to the vehicle. When a vehicle is in junction mode, it compares its buffer occupancy with threshold δ. If the buffer occupancy is higher than δ, it broadcasts an Alarm message. When surrounding vehicles receive the message, they ignore the vehicle when using packet forwarding algorithm.

D. Proxy CAM

In CITS, a CITS enabled vehicle can detect vehicles which transmit CAMs and can be captured by the vehicle's sensors. However, IEEE 802.11p is weak to obstacles and it can be blocked by buildings easily. This creates a type of blind spot that no vehicle can be detected by either the sensors or CAMs, which can contribute to an accident. Additionally, there are vehicles that are not CITS-enabled. These vehicles need to be detectable by CITS-enabled vehicles. To solve this problem, [16] proposed Proxy CAM system, which installs computer vision sensors at the roadside and leveraging images captured by them. A server detects the vehicles by

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-643-9

the images and makes CAMs for them and broadcasts them from transmitters installed at the roadside using IEEE 802.11p. In our previous work, we proposed Remote Proxy CAM [4], which delivers CAMs over the Internet using UDP/IPv6 and LTE with standard specification (i.e., basic transportation protocol/geonetworking and IEEE 802.11p).

IV. Problem Statement

In this section, we analyze the problems of Proxy CAM system. There are four problems: short wireless range, low fault tolerance, inefficient routing, and tradeoff between wide transmission and traffic load. We describe them in detail below.

A. Short wireless range

In [17], the Packet Delivery Ratio (PDR) of a vehicle traveling at 20 km/h using IEEE 802.11p with a data rate is 12 MB/s was nearly 100% when the range was to 700 m. However, this experiment was done in the flat plains with no buildings around and nearly no other wireless communication. However, in urban areas, there are buildings and other wireless communication. This environment can cause multipath propagation and wave interference. Thus, in this environment, the wireless range of IEEE 802.11p will diminish. Also, this Proxy CAMs can be used to determine the density of intersections. This information is very valuable to many applications, such as navigation for avoiding traffic jams. So, Proxy CAMs need to be provided enough early and this makes the problem of how to make the transmission far enough.

B. Low fault tolerance

IEEE 802.11p uses a relatively high-frequency bandwidth, 5.9 GHz. And this makes it weak to obstacles. Proxy CAM system overcomes this problem by installing transmitters around intersections. However, if the road connected to the intersection is curvilinear or if there is a large track, it may interrupt the communication between the Proxy CAM device and a vehicle. This interruption may be temporal, but for safety, it is a critical hazard.

C. Inefficient routing

Described in short wireless range, there is an unavoidable case that a vehicle needs far Proxy CAMs and cannot get them because of the communication range of IEEE 802.11p. To solve this problem, one solution is to relay the Proxy CAM packets. The devices to relay and broadcast the packets (i.e., transmitters) can be vehicles or RSUs. This relaying the packets adds the problem of how to perform the routing control. This routing control includes identifying devices for relaying, and how far Proxy CAM packets need to be relayed. Additionally, there are road traffic-related factors, such as traffic volume, accident rate in the past, and time-of-day. This routing must consider these factors and provide alternate routing for each Proxy CAM device.

D. Trade-off between wide transmission and traffic load

Described before, it needs to lengthen the communication range of Proxy CAMs to improve the safety. And to do this, relaying Proxy CAM packets and transmitting from a remote transmitter is the solution. However, for the transmitter, if the range is too long, the number of the Proxy CAM devices that use this transmitter increases dramatically. This means the number of the Proxy CAM packets also increases. For wired communication, the amount of the traffic load is small, but for wireless communication, especially IEEE 802.11p, the bit rate is 3∼27 MB/s and this is used for broadcasting Proxy CAM packets to vehicles in Proxy CAM system. Thus, if the amount of Proxy CAM packets is too high, the transmitter cannot handle the packets and this makes packet loss and delay.

V. Grid Proxy CAM

To solve the problems in the previous chapter, we propose Grid Proxy CAM system. This system is basically composed of Proxy CAM device and relaying devices. In inefficient routing problem described in the previous chapter, this problem would be solved by relaying the packets, and devices to relay the Proxy CAM packets can be vehicles or RSUs. In [15], they used vehicles. Unfortunately, this method depended on vehicle speed and density, and these factors change quickly in the real world. The quality of safety-related services must always be high, and the extant proposals were not suitable for relaying Proxy CAM packets. So in this study, we use RSUs as the relaying devices that are routers installed at each intersection with a Proxy CAM device. For the problems of inefficient routing and the trade-off between wide transmission and traffic load, we have been developing two methods: SDN routing and Passive selection.

A. SDN routing

Figure 1 shows the overview of SDN routing method. This method uses SDN for routing, and all routers relay the Proxy CAM packets by following their SDN flow table. Each Proxy CAM device is composed of a Proxy CAM generator that detects surrounding vehicles with computer vision and generates their Proxy CAMs, and a Proxy CAM transmitter that broadcasts Proxy CAMs using IEEE 802.11p. These generators and transmitters are connected to each router, and adjacent routers are also connected. Each router connected to an SDN controller. These connection are wired, and all Proxy CAM generators, transmitters, routers, and the SDN controller have an IP address and communication between generators, transmitters, and routers use UDP.

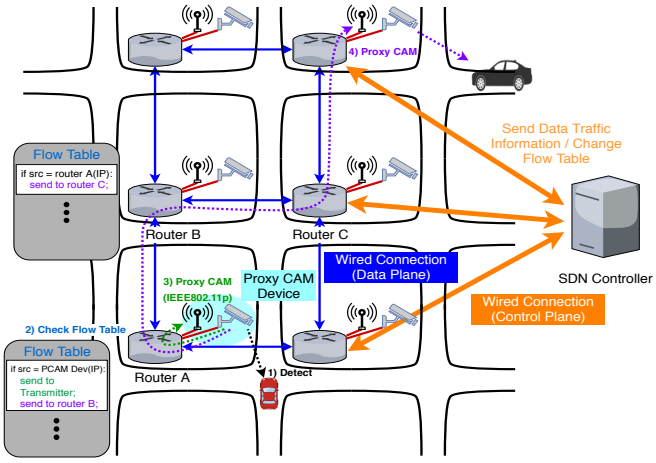

Figure 1. Overview of Grid Proxy CAM with SDN routing.

The SDN controller changes the flow entries of each router's flow table periodically according to the traffic load

of each transmitter which is connected to the router, and the priority. This priority indicates how important Proxy CAMs generated by the directly connected Proxy CAM generator are to road safety. The factors for determining this priority includes the type of the street where the Proxy CAM device is installed (i.e., the street is the main street or not), the accident rate in the past, whether the street is curvilinear and it is difficult to see far, the density of vehicles, whether there is a fast moving vehicle that can cause an accident, and whether there is an emergency vehicle. With the traffic load and the priority, the SDN controller changes the flow entries so that each transmitter can broadcast as many Proxy CAM packets as possible. However, their amount does not exceed the capacity of the transmitter's IEEE 802.11p limitations.

The procedure is as follows.

1) A Proxy CAM generator detects surrounding vehicles and generates Proxy CAMs and sends to a connected router.
2) When the router receives the packets, it checks its SDN flow table and follows instructions. By default, in this flow table, there is an entry that checks if the Proxy CAM packets are from the directly connected Proxy CAM generator, sending them to the directly connected transmitter. Additionally, the SDN controller can add and delete flow entries to duplicate the packets and sends them to adjacent routers.
3) The directly connected transmitter broadcasts the packets with IEEE 802.11p as soon as it receives the packets.
4) The router also has the flow entries for incoming packets from neighbor routers, used to duplicate the packets and send to adjacent routers and the directly connected transmitter.

During this procedure, the SDN controller always gets necessary information from routers and periodically changes flow entries of each router.

B. Passive selection

Figure 2 shows the overview of passive selection method. The hardware architecture of this method is very similar to SDN routing. There are routers and Proxy CAM generators and Proxy CAM transmitters. Each Proxy CAM generator and Proxy CAM transmitter is connected to a router, and the router is connected to adjacent routers. These connections are wired and use UDP/IP protocol. Transmitters broadcast Proxy CAM packets using IEEE 802.11p. In this method, we assume that communication speed of wired connections is enough high and the data load of Proxy CAM packets does not occupy the bandwidth. Each router has a geographical range and it receives Proxy CAM packets from routers which are within the range. In detail, each router has a list of other routers' IP addresses which are within the range in advance, and the routing is done with RIP or OSPF, which are legacy network's protocols. With the IP address list, each router sends Proxy CAM packets.

When a router receives Proxy CAM packets, it duplicates them and sends to the next routers and to a directly connected transmitter. The transmitter checks the number of packets. If it is less than the bandwidth of IEEE 802.11p, it broadcasts all the packets using IEEE 802.11p. However, if the number is more than the bandwidth, it is impossible to send all of them. Thus, the transmitter selects the Proxy CAM and broadcasts the selected packets. The factors for how to select the packets would be the geographical distance to the original Proxy CAM device, the street on which the original Proxy CAM device is installed is the main street or not, the street is curvilinear or not, the density of vehicles, if there is a fast-moving vehicle, and if there is an emergency vehicle.

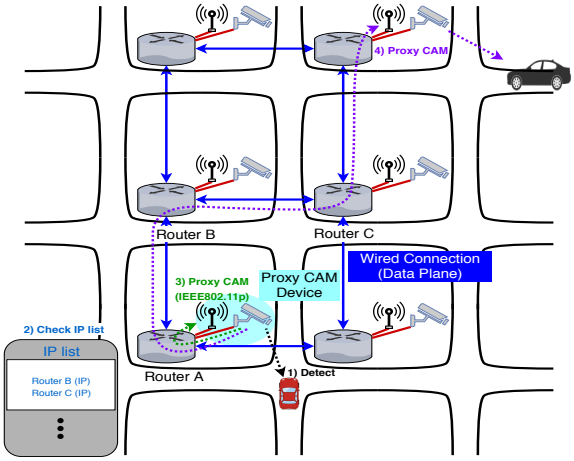

Figure 2. Overview of Grid Proxy CAM with Passive selection.

The procedure is as follows.

1) A Proxy CAM generator detects the surrounding vehicles and generates Proxy CAMs and sends to a connected router.
2) When the router receives the packets, it checks its IP list and sends the packets to the routers listed. The routes to them are established using the original network protocols. Additionally, it sends the packets to the directly connected transmitter.
3) The directly connected transmitter broadcasts the packets using IEEE 802.11p as soon as it receives the packets.
4) The transmitter also broadcasts the packets from other Proxy CAM generators. However, if the data load of the packets exceeds the capacity of IEEE 802.11p, it selects the packets and drops the rest.

VI. Conclusions and Future Work

In this paper, we proposed Grid Proxy CAM system that uses RSUs as routers. Each router is connected to Proxy CAM generator, transmitter, and also neighboring routers. We introduced two methods of SDN routing and passive selection that forward Proxy CAM packets and control their load.

SDN routing makes the route control easy and dynamic. This makes the system flexible to network and situational changes (e.g., when a new road is built or an existing road is extended). Additionally, all routes are defined by an SDN controller and the controller defines only the necessary routes. Thus, the load to not only IEEE 802.11p that transmitters use but also every wired connection in this system should be minimum. In addition to these points, routers and transmitters are not given some heavy task to handle the packets. This means their performance can be low. Thus, the price for the

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-643-9

system can be low. On the other hand, SDN routing is done by an SDN controller. This routing process can still be heavy. Thus, the controller must be high-performance. Additionally, if a failure occurs to the controller, all routers cannot change the routes, which may cause the system to stop.

Passive selection is a decentralized system. This means there is no single point of failure. Thus, this system is strong. Additionally, this method does not require complex tasks and uses legacy network technology. Thus, it is easy to install. On the other hand, passive selection is not as flexible as SDN routing. It requires manual operation to change IP address lists and the range of getting Proxy CAM. Additionally, this system requires transmitters to select the packets. If this process takes time, the property of real-time may be lost.

We are also considering that our previous work, Remote Proxy CAM [4] can be combined with this Grid Proxy CAM. The remote Proxy CAM system is composed of Proxy CAM devices and a server. Vehicles can access the server by sending a request with their position via LTE and can get Proxy CAM information. When the server receives a request, it checks the position of the source vehicle and gathers the Proxy CAM from routers that are within a certain range from the vehicle. It then sends them to the vehicle. In this system, vehicles use LTE to communicate, and this wireless technology covers almost every location in the city. Thus, theoretically, vehicles can get all information from Proxy CAM devices in the city. With this different characteristic, we are considering Grid Remote Proxy CAM system that uses Grid Proxy CAM system for collecting nearby Proxy CAMs and Remote Proxy CAM for collecting remote Proxy CAMs. This combined system will use both IEEE 802.11p and LTE. This means this system disperses the network traffic load and is also strong to radio wave interference.

For future work, we plan to propose algorithms of SDN controller's altering flow entries and passive selection's selecting incoming packets. Additionally, we will implement this system in a network simulator and perform experiments. With the outcome of these experiments, we will discuss the effect of the methods. In addition to this, we will implement the combined Grid Remote Proxy CAM system and examine how much this system improves safety.

ACKNOWLEDGEMENT

This work was partly supported by JSPS KAKENHI Grant Number JP17H04678.

REFERENCES

[1] ProPILOT, retrieved: 06, 2018. [Online]. Available: https://www.nissan-global.com/JP/TECHNOLOGY/OVERVIEW/propilot.html

[2] ETSI, "TR 102 962 - V1.1.1 - Intelligent Transport Systems (ITS); Framework for Public Mobile Networks in Cooperative ITS (C-ITS)," 2012, retrieved: 06, 2018. [Online]. Available: http://www.etsi.org/deliver/etsi_tr/102900_102999/102962/01.01.01_60/tr_102962v010101p.pdf

[3] IEEE Computer Society. LAN/MAN Standards Committee., Institute of Electrical and Electronics Engineers., and IEEE-SA Standards Board., IEEE standard for Information technology– telecommunications and information exchange between systems– local and metropolitan area networks– specific requirements : Part 11 : Wireless LAN medium access control (MAC) and physical layer (PHY) specifications : Amendment 6: Wireless access in vehicular environments. Institute of Electrical and Electronics Engineers, 2010, retrieved: 06, 2018. [Online]. Available: http://ieeexplore.ieee.org/document/5514475/

[4] M. Kitazawa, M. Tsukada, K. Morino, H. Ochiai, and H. Esaki, "Remote Proxy V2V Messaging using IPv6 and GeoNetworking," in The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications (VEHICULAR 2017), July 2017, pp. 74–80, retrieved: 06, 2018. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01578410

[5] Its, "EN 302 636-5-1 - V1.2.0 - Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol," retrieved: 06, 2018. [Online]. Available: http://www.etsi.org/deliver/etsi_en/302600_302699/3026360501/01.02.00_20/en_3026360501v010200a.pdf

[6] ——, "TS 102 636-4-1 - V1.1.1 - Intelligent Transport Systems (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality," retrieved: 06, 2018. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/102600_102699/1026360401/01.01.01_60/ts_1026360401v010101p.pdf

[7] ETSI, "EN 302 637-2 - V1.3.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," retrieved: 06, 2018. [Online]. Available: http://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.03.02_60/en_30263702v010302p.pdf

[8] ETSI EN 302 637-3 v1.2.2(2014-11), Intelligent Transport Systems(ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service, 2014, retrieved: 06, 2018. [Online]. Available: http://www.etsi.org/deliver/etsi_en/302600_302699/30263703/01.02.02_60/en_30263703v010202p.pdf

[9] Software-Defined Networking (SDN) Definition, retrieved: 06, 2018. [Online]. Available: https://www.opennetworking.org/sdn-definition/

[10] M. Torrent-Moreno, P. Santi, and H. Hartenstein, "Fair sharing of bandwidth in VANETs," in Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks - VANET '05. New York, New York, USA: ACM Press, 2005, p. 49.

[11] K. Zrar Ghafoor, K. AbuBakar, M. van Eenennaam, R. H. Khokhar, and A. J. Gonzalez, "A fuzzy logic approach to beaconing for vehicular ad hoc networks," Telecommunication Systems, vol. 52, no. 1, January 2013, pp. 139–149.

[12] K. Suriyapaibonwattana and C. Pomavalai, "An Effective Safety Alert Broadcast Algorithm for VANET," in 2008 International Symposium on Communications and Information Technologies. IEEE, October 2008, pp. 247–250.

[13] B. Liu, D. Jia, J. Wang, K. Lu, and L. Wu, "Cloud-Assisted Safety Message Dissemination in VANETCellular Heterogeneous Wireless Network," IEEE Systems Journal, vol. 11, no. 1, March 2017, pp. 128–139.

[14] I. Ku et al., "Towards software-defined VANET: Architecture and services," in 2014 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET). IEEE, June 2014, pp. 103–110.

[15] X. Ji, H. Yu, G. Fan, and W. Fu, "SDGR: An SDN-Based Geographic Routing Protocol for VANET," in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, December 2016, pp. 276–281.

[16] T. Kitazato, M. Tsukada, H. Ochiai, and H. Esaki, "Proxy cooperative awareness message: an infrastructure-assisted v2v messaging," in 2016 Ninth International Conference on Mobile Computing and Ubiquitous Networking (ICMU), October 2016, pp. 1–6, retrieved: 06, 2018. [Online]. Available: http://ieeexplore.ieee.org/document/7742092/

[17] O. Shagdar, M. Tsukada, M. Kakiuchi, T. Toukabri, and T. Ernst, "Experimentation towards ipv6 over ieee 802.11p with its station architecture," in International Workshop on IPv6-based Vehicular Networks, June 2012, pp. 1–6, retrieved: 06, 2018. [Online]. Available: https://hal.archives-ouvertes.fr/hal-00702923

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-643-9