International Journal of Multimedia and Ubiquitous Engineering
Vol. 9, No. 12 (2014), pp. 383-404
http://dx.doi.org/10.14257/ijmue.2014.9.12.34

Message Propagation based on Three Types of Density Classification for Smooth and Secure Vehicular Traffic Flow

ByungKwan Lee[1], EunHee Jeong[2] and YiNa Jeong[3]

[1]Dept. of Computer, Catholic Kwandong University
[2]Dept. of Regional Economics, Kangwon National University
[3]Dept. of Computer, Catholic Kwandong University
E-mail: bklee@cku.ac.kr, jeongeh@kangwon.ac.kr, lupinus77@nate.com

Abstract

This paper proposes Message Propagation based on Three types of Density Classification for Smooth and Secure Vehicular Traffic Flow. The Message Propagation based on Three types of Density Classification (MPTDC) measures the density on three types of roads, namely a secluded rural road (0), a highway (1), and a urban intersection (2) and propagates messages to each classified one. When the type of message propagation is 1 and 2, the MPTDC generates a Cluster key by using MAC after grouping vehicles into a Cluster. The Cluster Header aggregates traffic information, and transfers it to a destination after filtering redundant or tampered traffic information. When the type of message propagation is 0, the MPTDC transfers traffic information by using RSU without generating a Cluster. In particular, when the type of message propagation is 2, the MPTDC selects a transmission path according to the density. Hence, this paper not only provides efficient communication but also improves the reliability of messages because it aggregates frequently encountered redundant messages.

Keywords: *VANET, Cluster Key, Aggregation, Density classification, Message Authentication Code*

1. Introduction

Recently Intelligent Transportation System (ITS) is being studied to build a safe and efficient Smart Highway The it provides not only commercial service in real time such as traffic information, digital map, and music through Vehicle to Infrastructure (V2I) but also driver's secure information services such as vehicle collision avoidance and accident alarm through Vehicle-to- Vehicle (V2V) [1]. However, VANET does not satisfy both communication efficiency and security at the same time [1, 2].

This paper proposes the Message Propagation based on Three types of Density Classification (MPTDC) to tackle these two problems. It measures the density on three types of roads, namely a secluded rural road, a highway, and a urban intersection and propagates messages to each classified one. The Cluster Header aggregates traffic information, and transfers it to a destination after filtering redundant or tampered traffic information. Hence, this paper not only provides efficient and secure communication but also improves the reliability of messages because it aggregates frequently encountered redundant messages.

[1] First author : ByungKwan Lee, Catholic Kwandong University
[2] Corresponding author : EunHee Jeong, Kangwon National University

ISSN: 1975-0080 IJMUE

The remainder of this paper is organized as follows. Chapter 2 discusses the related works. Chapter 3 designs the MPTDC technique. Chapter 4 analyzes the MPTDC, and finally in Chapter 5, our conclusion is described.

2. Related Works

2.1 Vehicular Communication System

Vehicular communication system consists of On Board Unit (OBU), Road Side Unit (RSU) and service infrastructure. Figure 1 shows the components of Vehicular Communication System and inter-vehicle communication [2, 3].

The OBU is a system which is installed inside a vehicle to support inter-vehicle communication. The OBU consists of Sensors, a Routing Table (RT), a Local Dynamic MAP (LDM), a Communication Control Unit (CCU) and an Electronic Control Unit (ECU). Here, Sensors sense every information which is related to driving of vehicle, the RT has the location information of neighboring vehicle, and the LDM is a MAP database which reflects traffic information and road status information near a vehicle. The CCU is a module to connect a vehicle within a group to that outside the group for communication. The ECU manages the sensors which are located within the vehicle and controls engine status, automatic transmission, and so on by using a computer.

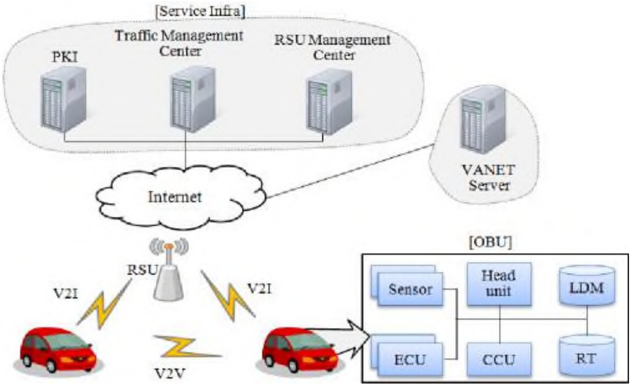


Figure 1. The Vehicular Communication System

The service infrastructure consists of Public Key Infrastructure (PKI), traffic management center, and RSU management center and uses a wire network [3].

2.2 VANET

A Vehicular Ad hoc Network (VANET) provides convenient wireless network services. In addition, in VANET, vehicles can exchange and receive the traffic information [4, 5]. VANET can enhance traffic safety and improve traffic efficiency [6, 7] by transmitting the messages with traffic information and road condition information. Hence, traffic accidents and jams can be significantly diminished. Since inexpensive wireless devices are available, they can be installed at various RSUs, such as road signs and traffic lights. Two communications, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, can take place in VANET [8].

The primary objective of VANET is to provide real-time exchange of messages between vehicles to ensure safety. However, the security of VANET is important because messages can be tampered or counterfeited by malicious nodes during transmission [8-10].

Research on VANET security is abundant [11-19]. Fujii [20] proposed an efficient group signature scheme in which he introduced a subscription service model. The scheme was useful for anonymous authentication and subscription service. Sun [21] proposed an efficient Distributed Key Management scheme (DKM) for group signature in VANET to solve the huge revocation overhead. The DKM could decrease the revocation cost. However, a malicious user might utilize the excellent anonymity property of group signature to send out forged message to other vehicles. Zhang [22] introduced the system architecture, applications and categories of attacks in VANET and summarized several types of anonymous authentication techniques, including pseudonym, random silence, group signature, ring signature, blind signature, and smart card which focused on protecting the privacy of vehicular nodes and could be good solutions for privacy protection. To solve the storage problem in a large number of anonymous certificates and the delay problem in group signature [23].

The basic idea of group based schemes is employing a group to hide the group member, then the real identity is covered and the privacy is protected. In [14], Lin, *et al.*, suggested a privacy preserving authentication scheme based on Group Signature [24, 25] and Identity (ID)-based Signature [26] (GSIS). In group signature, a message is anonymously signed by a private key of a sender and verified by the group public key, while identities of senders can only be recovered by authorities. ID-based signature is applied by RSUs to digitally sign each message launched by RSUs to ensure its authority, where the signature overhead can be greatly reduced. CRL size of group signature is linear with the number of revoked vehicles, but CRL checking operation involves two paring calculations, which would take about 104 times computation cost than a string comparison [27]. In [28], Zhang et al. employed each RSU to maintain and manage an on-the-fly group within its communication range. Vehicles entering the group can anonymously broadcast V2V messages, which can be instantly verified by the vehicles in the same group (and neighbor groups). Due to numerous RSUs sharing the load to maintain the system, performance does not significantly degrade when more vehicles join the VANET. But this scheme needs RSU to be pervasive otherwise the scheme is ineffective [29].

Obviously, although there are a lot of approaches in VANET system security authentications based on group signature and pseudonym, the majority of anonymous authentication schemes only provide the anonymity between different vehicles, but not between vehicles and RSUs, which cannot satisfy the system requirements of VANET.

On the other hands, a few of researches about propagation in VANET have been suggested. In SOTIS [30], vehicles on a road segment periodically send reports containing the traffic information on the current road segment. For each segment, average speed is calculated and then forwarded. During the broadcast interval, a vehicle collects and aggregates information received from neighboring vehicles. This approach helps generate an overview of current traffic conditions by periodical broadcasting of information. However, periodical report broadcasting is not an efficient way for report propagation, and there is no guarantee that redundant reports from the same road segment can be aggregated together. TrafficView [31] is another similar system which uses periodic report broadcasting for disseminating traffic information. Like SOTIS, it disseminates information about the average speed of vehicles on the roads. TrafficView differs from SOTIS in a way that it is node-centric i.e. messages of the nodes that are close to each other are aggregated by averaging their current speed and position. A list of all involved nodes is kept with the aggregate [32].

Sun and Garcia-Molina [33] have proposed bidirectional perimeter-based propagation of regional alerts for fast data delivery. However it does not consider the security of the data propagation. Zhao and Cao [34] have suggested an improved way for fast message routing in more complex roads using information about destination location, vehicle's location and moving direction. Rahman and Hengartner [35] have introduced the concept of cryptographically-verifiable road-worthiness certificates for secure crash reporting. That covers the security problems which can happen in the data propagation. However, it needs to operate additional governmental authorities and road-side access points to manage the certificates.

In order to provide secure communications and anonymous authentication among vehicles, this paper proposes the cluster key of vehicles, generates a signature of traffic information by using the cluster key, and verifies the signature. Also, this paper proposes the proper message propagation scheme according to the three types of density of roads. Hence, this paper not only provides secure communication and anonymous authentication but also improves efficiency by propagating the traffic information

3. MPTDC Design

3.1 System Overview

The proposed Message Propagation based on Three types of Density Classification (MPTDC) for Smooth and Secure Vehicular Traffic Flow consists of MPTDC Server, RSU, and Traffic Management Center in Figure 2. If vehicle ID is registered in the MPTDC Server, the MPTDC Server issues a System Key to a vehicle.

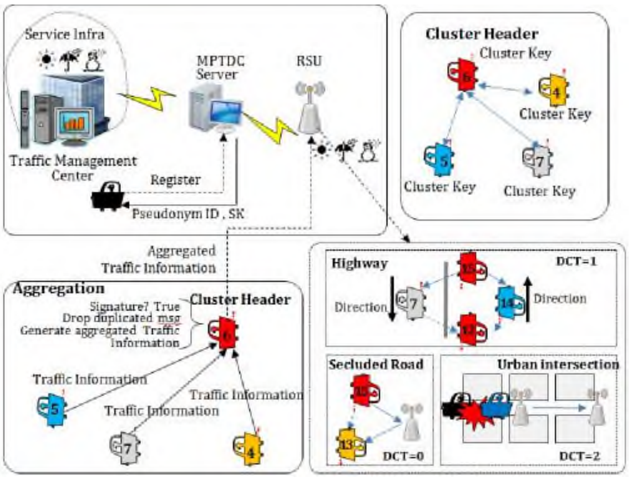


Figure 2. The Components of the MPTDC

To begin with, the MPTDC measures the density a road, generates a Cluster if the density is greater than a critical value, and selects a Cluster Header. The Cluster Header aggregates traffic information transferred from the vehicles within a Cluster.

The MPTDC generates a Cluster and a Cluster Header. Then the Cluster Header aggregates traffic information. At this time, the Cluster Header deletes the traffic information that does not match a signature and duplicate traffic information.

The MPTDC classifies roads into a secluded road, a highway, an urban intersection according to the Density Classification and provides a message propagation technique suitable for the classified type.

The MPTDC transfers the traffic information to a destination with this message propagation technique.

3.2 Cluster Generation

The MPTDC uses Algorithm 1 for the generation of a Cluster.

Algorithm 1. The generation of a Cluster

```
set a critical value "c" for the generation of a Cluster
define the range of a road
count the number of vehicles on a road
compute the density "d" of the road

check a moving direction "md"
   I
judge the generation of a Cluster by using "d" and
      "md" {
```

The MPTDC decides a critical value "c" and computes density "d" by the following expression.

In case the moving direction of vehicles is different, the MPTDC sets "md" as 0. In case the moving direction of vehicles is the same, the MPTDC sets "md" as 1 in Algorithm 1. Finally, The MPTDC generates a Cluster in case the following expression is true.

{

3.3. Cluster Key Generation

The MPTDC selects a Cluster header and generates a Cluster Key in Algorithm 2. Figure 3 shows the process that the Cluster Key is generated.

Algorithm 2. Cluster Key generation

```
Identify a Road Number($R_N$)
The first vehicle is selected as a Temporary Cluster Header (TCH)
The TCH generates nonce using by random function and calculates MAC and NS.
    Nonce = rand()
    MAC = H($R_N$ || SK || nonce)
    NS = nonce □ SK
The TCH broadcasts the MAC and the NS to The vehicles in the cluster.
The vehicles decrypt nonce and calculates MAC′
    NS = nonce □ SK
    MAC′ = H($R_N$ || SK || nonce)
```

```
6:  The vehicles verify the MAC which is received from the TCH as

     follows. I

7:  If V(verification) is 0, the vehicles drop the MAC
8:  If V is 1, the vehicles transfer Pseudonym ID (PID) and a Public Key (PK) to the TCH.
9:  The TCH generate a Neighboring List (Nlist) and calculates Sum of a Public key (SP).
     Nlist = {V16, V15, V14, V13, V12}
     SP = PK16 + PK15 + PK14 + PK13 + PK12
10: The TCH broadcasts the Nlist and the SP to the vehicles in the cluster.
11: the vehicles identify the Nlist.

        {

12: If NC (Neighboring Check) is 0, the vehicles drop the Nlist and the SP.
13: If NC is 1, the vehicles calculate a Cluster Key
     Cluster = SP + SK
14: The TCH selects as a Cluster Header the vehicle which is located farthest and broadcasts the
     CH encrypted by XORing PID and Cluster Key to vehicles
     CH = PID  Cluster Key
15: The vehicles decrypt the CH and recognize the PID of a Cluster Header.
     PID = CH  Cluster Key
```

The MPTDC checks a Road Number (R_N) in Figure 3(a) and selects a Temporary Cluster Header (TCH). The TCH generates nonce by rand() function in Figure 3(b) and calculates MAC and NS with the following expressions.

Nonce = rand()
MAC = H(R_N || SK || nonce)
NS = nonce SK

Here, SK is a system key issued from the MPTDC Server. The vehicles within a Cluster compute MAC′ after decrypting the NS. At this time, Verification (V) value is decided with the following expression.

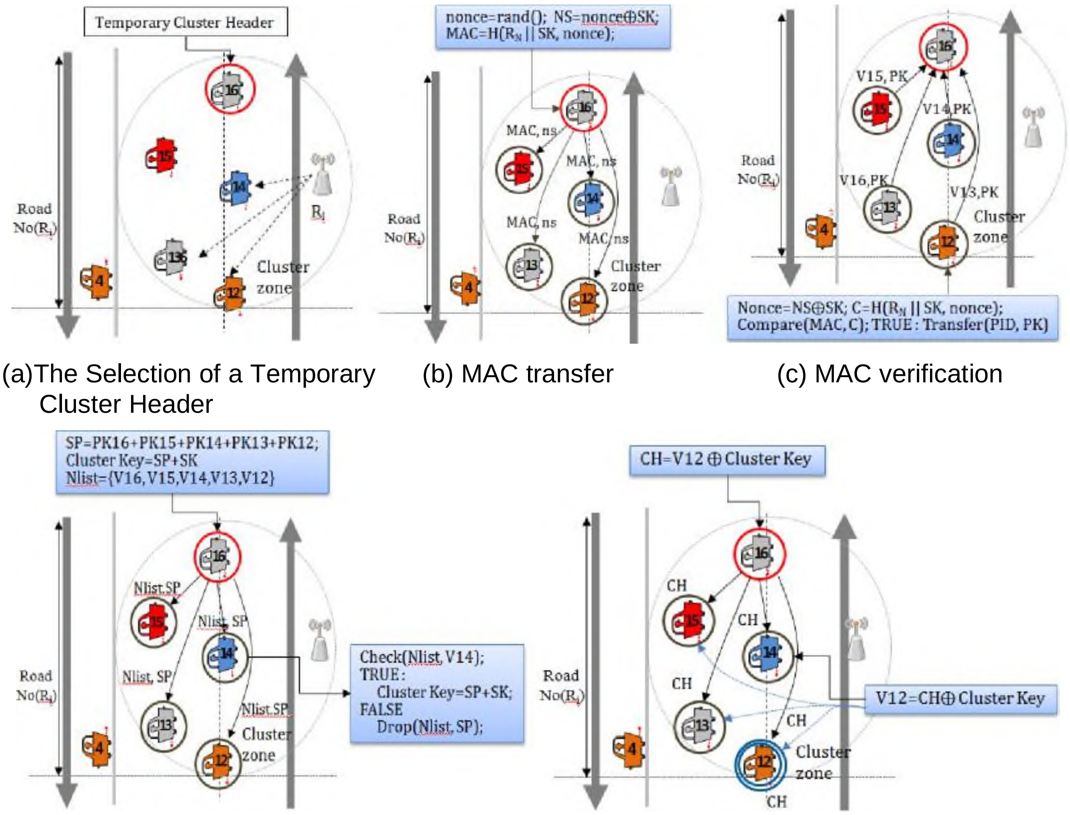
I

In Figure 3(d) the TCH generates the Nlist with the PID of vehicles and computes the SP (Sum of Public key) with the public keys by the following expressions. The TCH broadcasts the Nlist and the SP to the vehicles within a Cluster.

Nlist = {V16, V15, V14, V13, V12}
SP = PK16 + PK15 + PK14 + PK13 + PK12

The vehicles which received the Nlist and the SP confirm that their PIDs are included in the Nlist with the following expressions.

{



(a)The Selection of a Temporary Cluster Header (b) MAC transfer (c) MAC verification

(d) The generation of a Cluster Key (e) The selection of a Cluster Header

Figure 3. The Selection of a Cluster and a Cluster Header

The vehicles drops the Nlist and the SP if NC=0, and computes a Cluster Key by assigning the SP and SK to the following expression if NC=1.

Cluster = SP + SK

In Figure 3(f), the TCH generates CH by assigning the PID and the Cluster Key to the following expression in order to inform that the vehicle which is located farthest is a Cluster Header. The TCH broadcasts the CH to the vehicles within cluster.

CH = PID Cluster Key

The vehicles which received the CH decrypt a Cluster Key and confirm the PID of a Cluster Header. Therefore, the MPTDC generates a Cluster Key by Algorithm 2 and selects a cluster header.

3.4 Aggregation Procedure based on Signature and Integrity

The MPTDC generates Aggregated Traffic Information (ATI) by Algorithm 3. Figure 4 shows the process that the MPTDC aggregates traffic information.

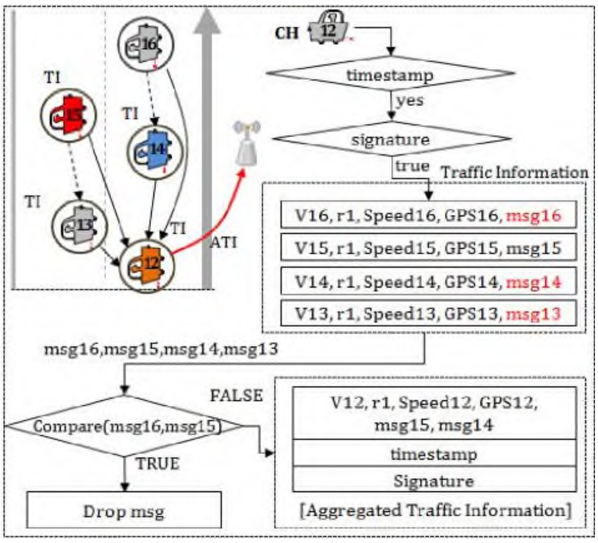


Figure 4. The Process of Message Aggregation

Algorithm 3. Aggregation

```
Create Traffic Information(TI)
Transfer TI to Cluster Header
Cluster Header checks the timestamp of TI.
    {
    if T(Timestamp) is 0, Cluster Header drops the TI
    if T is 1, Cluster Header verifies signature of TI
        {
        if S(signature) is 0, Cluster Header drops the TI
        if S is 1, Cluster Header compares the msg of TI.
            {
            if Dup (duplication) is 0, Cluster Header aggregates msg into AT I(Aggregated Traffic
               Information).
            if Dup is 1, Cluster Header drops TI
Cluster Header generates signature of ATI using by SK.
```

In Figure 5 vehicles generates the traffic information signed by a Cluster Key and transfers it to a Cluster Header.

The Cluster Header confirms that the timestamp (T) of traffic information is valid. In case T is 1, the Cluster Header generates the signature′ by assigning all the information except the signature in traffic information in Figure 5 and the Cluster Key (CK) to the following expression.

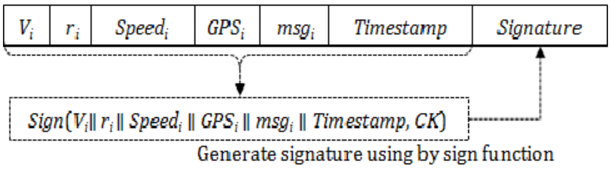

V_i
r_i
$Speed_i$
GPS_i
msg_i
$Timestamp$
$Signature$
$Sign(V_i \| r_i \| Speed_i \| GPS_i \| msg_i \| Timestamp, CK)$
Generate signature using by sign function

Figure 5. Traffic Information (TI)

The Cluster Header compares the signature′ to the Signature of traffic information and stores the result in S. If S=0, it drops TI because TI is traffic information which is forged. If S=1, the Cluster Header confirms that traffic message msg is duplicate by using the following expression. If it is true, it drops the traffic information.

$$\{$$

Therefore, the Cluster Header collects just the msg that the signature matches and is not duplicated and generates the Aggregated Traffic Information (ATI) in Figure 6. At this time, the Cluster Header generates the signature with the System Key (SK) that the MPTDC Server issued.

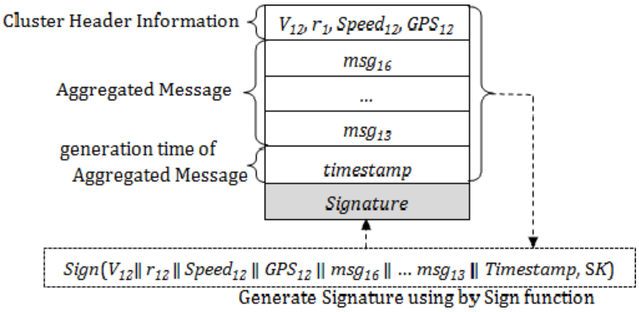

Cluster Header Information
Aggregated Message
generation time of Aggregated Message
$V_{12}, r_1, Speed_{12}, GPS_{12}$
msg_{16}
...
msg_{13}
$timestamp$
$Signature$
$Sign(V_{12} \| r_{12} \| Speed_{12} \| GPS_{12} \| msg_{16} \| \ldots msg_{13} \| Timestamp, SK)$
Generate Signature using by Sign function

Figure 6. The Structure of ATI

3.4 Density Classification

In an inter-vehicle communication, because the traffic information influences the following vehicle's safety and traffic flow, it must be propagated rapidly and safely.

The MPTDC computes density by Algorithm 4 and Density Classification Type (DCT) is decided according to the result.

Algorithm 4. Density Classification Type

```
1: Define the range of a road
2: Count the number of vehicles in road
3: Set critical value "c" for DCT
4: Compute density "d" of road

5: Confirm the position of vehicle
      {
```

6: Check the DCT

I

To begin with, the MPTDC sets a critical value (c) for the decision of DCT and computes the density of a road by the following expression.

After the MPTDC confirms the location of vehicles, it sets the location value to the following expression u.

{

It decides the DCT by assigning d, c, and u to the following expression.

I

Therefore, the MPTDC classifies roads into a Secluded Road (DCT=0), a Highway (DCT=1), and a Urban Intersection (DCT=2) and transfers traffic information with the message propagation method suitable for each DCT.

3.4.1 DCT=0(In Case of a Secluded Road)

It is difficult to transfer TI in the rural Road in which vehicles are secluded. In this case this paper propagates it safely by transferring TI to the following vehicles, RSU, and the vehicles moving in the opposite direction.

In a Secluded Road the process of traffic information propagation is as follows.

A source vehicle broadcasts TI to the following vehicles, RSU, and the vehicles moving in the opposite direction. After critical time, the source vehicle broadcasts TI to the following vehicles, RSU, and the vehicles moving in the opposite direction once more.

The vehicles and the RSU transfer them to a destination by delivering traffic information TI_1 and TI_2 to the following vehicles.

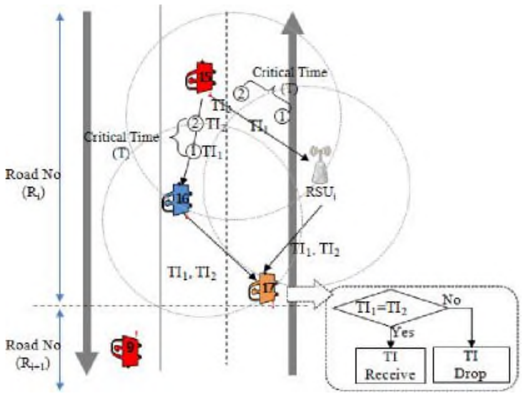


Figure 7. The Traffic Propagation in a Secluded Road and its Verification Procedure

That is, this propagation method is the more accurate because it transfers TI to the following vehicles more than twice and filters the forged TI by verifying the transferred TI.

3.4.2 DCT=1(In Case of a Highway)

In a Highway where vehicle movement is frequent in Figure 8, TI is securely propagated to both the following vehicles and those moving in the opposite direction at the same time.

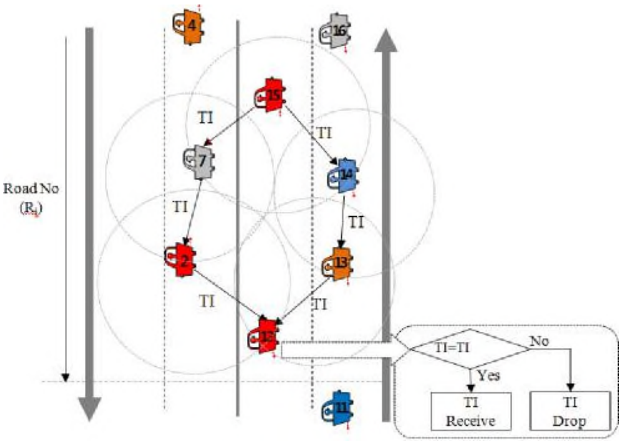


Figure 8. The Traffic Propagation in a Highway and its Verification Procedure

The process of TI propagation is as follows.

A source vehicle broadcasts TI to both the following vehicle 14 and the vehicle 7 moving in the opposite direction. The vehicle that received TI propagates it to the following vehicle 13 and the vehicle 7 propagates it to the preceding vehicle 2. Therefore, the destination vehicle 12 that received TI also receives it from the vehicle 2 and 13 at the same time. The destination vehicle 12 verifies that both two TI's matches. If they match, the TI is accepted. If they do not match, it is dropped.

That is, this propagation method not only catches traffic flow rapidly because the destination vehicle transfers TI in both direction but also filters the forged TI because the transferred TI is verified.

3.4.3 DCT=2 (In Case of an Urban Intersection)

In an Urban Intersection unlike a Highway, because a variety of variables such as Traffic accident, traffic control, etc can happen, this paper proposes to transfer Traffic Information speedily and accurately through the RSU's installed in every road section.

Table 1 is an essential element for the RSU installed in an urban intersection to transfer smooth traffic information.

The Information Table 1(a) has the RSU ID, RSU location, the road information and the weather information transferred from the Traffic Management Center. The Neighbor Information Table 1(b) has the Neighbor RSU ID, the Neighbor RSU location, and the road density about a neighbor. Vehicle Direction Table 1(c) has the direction about the location of the vehicles which received an Accident Notification Message). In particular, it is assumed that the Neighbor RSU information in the Neighbor Information Table among these tables is provided by RSU management center.

Table 1. RSU Table

(a) Information Table

Field	Contents
ID	RSU ID
location	RSU location
road	road information
weather	weather information

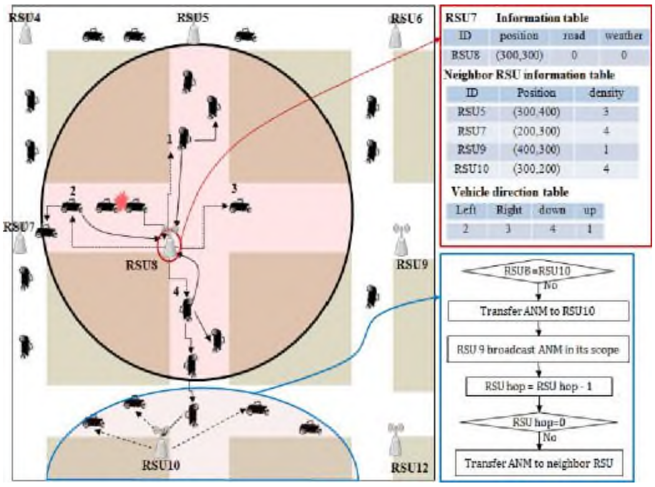
(b) Neighbor Information Table

Field	Contents
ID	neighbor RSU ID
location	neighbor RSU location
density	road density

(

Field	Contents
Left	vehicles in the (X-,Y0) direction
right	vehicles in the (X+,Y0) direction
down	vehicles in the (X0,Y-) direction
Up	vehicles in the (X0,Y+) direction

Figure 9 shows the process that the ANM is transferred to Neighbor RSU by the vehicles in an Urban Intersection. In case of an accident occurrence in an Urban Intersection, the accident vehicle and the neighboring vehicles transfer the accident information to the vehicles belonging to the RSU. At this time, the vehicles generate Accident Occurrence Message (AOM) like Figure 2 and transfer it to the RSU. The RSU which received the AOM generates Accident Notification Message (ANM) like Table 3 and transfers it to the Neighboring RSU. In Figure 9 the RSU 8 generates ANM and transfers it to the neighboring RSU. At this time, the RSU 8 transfers the ANM with RSU hop=2 to the vehicle 1, 2, 3, 4 within the transferring scope of the RSU 8.



RSU7 Information table

ID	position	road	weather
RSU8	(300,300)	0	0

Neighbor RSU information table

ID	Position	density
RSU5	(300,400)	3
RSU7	(200,300)	4
RSU9	(400,300)	1
RSU10	(300,200)	4

Vehicle direction table

Left	Right	down	up
2	3	4	1

Figure 9. RSU Table and Message Propagation Flowchart

Table 2. Accident Occurrence Message (AOM)

Field	Contents
Message ID	accident occurrence message= 01
Source IP Address	the IP Address of the vehicles which generated AOM
Destination IP Address	IP Address of the nearest RSU
level	accident level

The vehicle 1, 2, 3, 4 receives the ANM from the RSU8 and retransmits it to the neighboring vehicles again. The RSU8 decides that the broadcasting is successful if the ANM is returned from the vehicle 1,2,3,4 due to retransmission. The RSU8 writes in the Vehicle Direction Table the coordinate value of the node that succeeded in retransmitting the ANM.

For example, the vehicle 1 is written in the (X0, Y+), the vehicle 2 in the (X-, Y0), and the vehicle 4 in the (X0, Y-). At this time, because the vehicle 3 did not retransmit the ANM to other vehicles, the direction of the vehicle 3 is not written in the Vehicle Direction Table.

Table 3. Accident Notification Message (ANM)

Field	Contents
Message ID	ANM ID = 02
Source RSU ID	ANM generation RSU's ID
Message Sequence Number	ANM Sequence Number
Source IP Address	RSU's IP address within the scope of an accident
Forwarding Node_X	X coordinate of an intermediate vehicle
Forwarding Node_Y	Y coordinate of an intermediate vehicle
RSU hop	the transmission scope according to a risk

The vehicles that received the ANM compare the RSU ID which they belong to with the source RSU ID of the ANM. If they do not match, the vehicles decide that they are within the scope of another RSU. They transfer the ANM to the RSU belonging to them and do not broadcast it anymore. The RSU which received the ANM informs the vehicles within their scope of an accident occurrence in which source RSU ID is located. The RSU which received the ANM confirms RSU hop. If the RSU hop is not 0, the RSU which received the ANM inform its neighboring RSU of an accident occurrence until the RSU hop is 0 repeatedly. The RSU5, RSU7, and RSU10 receive the ANM according to the above procedure. But because the vehicle 3 did not have the neighboring ones, the RSU9 did not receive the ANM. Therefore, the RSU9 has to receive the ANM from the neighboring RSU5, RSU7, and RSU10. The proposed MPTDC selects an RSU that has the highest density among the RSU5, RSU7, and RSU10 stored in the Neighbor Information Table of the RSU8 and transfers the ANM to RSU9 rapidly.

4. Experimental Results

4.1 Experiments on Density Classification

The MPTDC proposed in this paper was experimented using an NS-2 simulator. The experiment considered the moving speed and direction of nodes and the simulation environment was shown in Table 4.

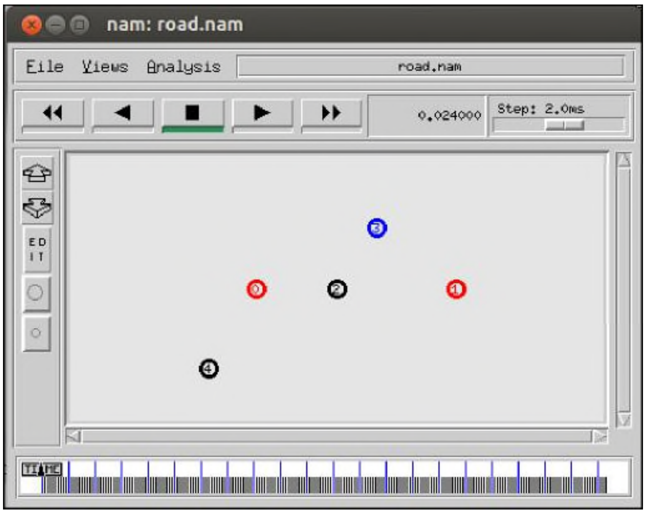
Table 4. The Simulation Environment

Parameter Name	Parameter Value	Parameter Name	Parameter Value
Protocol	AODV	Max. speed(m/s)	5
Simulation time	120 sec	Min. speed(m/s)	2
Simulation Area	1200×1200m	Packet type	TCP
Nodes numbers	5, 8, 34		
Transmission range	250m		

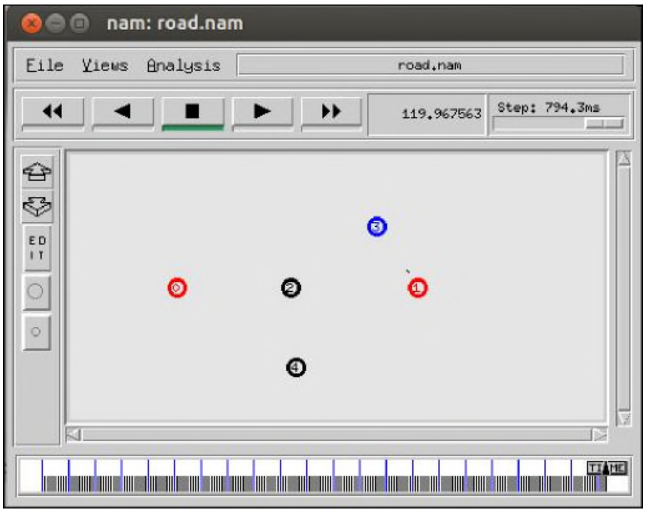
4.1.1 In case of DCT=0 (in a Secluded Road)

In the propagation simulation of Figure 12(a) where 4 nodes were deployed, the node 0 is set as a source node, the node 1 a destination node, and the node3 an RSU. The simulation had been executed for 120 seconds, the node0, 1 and 2 were moved to the left and node4 was moved to the right. The moved result was shown in Figure 12(b).

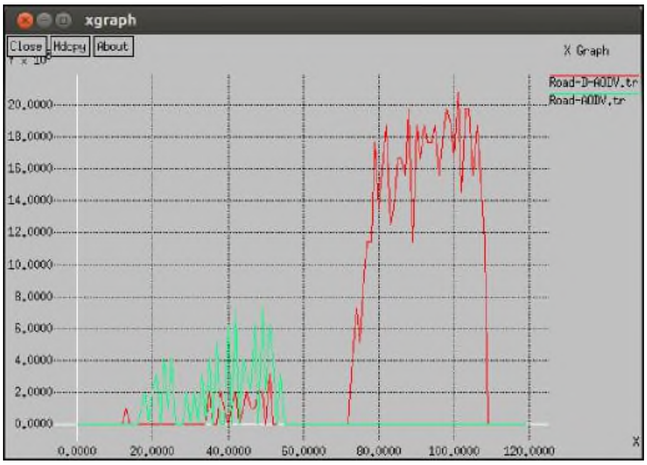
Because the node4 and node1 moved in the opposite direction, the node4 was excluded during simulation. Figure 12(c) shows the number of messages that the Node0 is propagating to the node1 for 120 seconds of the experiment. As shown in Figure 12(c), the message transmission path of the existing AODV is disconnected owing to node movement if the 60 seconds elapses in the experiment. Therefore, the existing AODV does not transfers messages to the destination if 55seconds elapses, but because in the propagation technique proposed in this paper, RSU propagates messages to the destination node 1 consistently; they can exactly be transferred to the node1.



(a) Before



(b) After



(c) The number of propagated message

Figure 12. Message Propagation in a Secluded Road

Table 5 shows the result of message propagation simulation by using 5 nodes in a Secluded Road. In the MPTDC, source nod 0 transfers messages to the node3 (RSU), and the node 3 transfers them to the nodes that enters the transmission scope of the node3 consistently. That is, as shown in Table 5, the number of messages transferred to the destination is increased in the node3 and when the node4 approaches the node1, messages are transferred.

Consequently, because the MPTDC transfers total 16,280 messages to the destination node1 and the number of messages that the destination node receives is 6,479, the message reception rate becomes 39.80%.

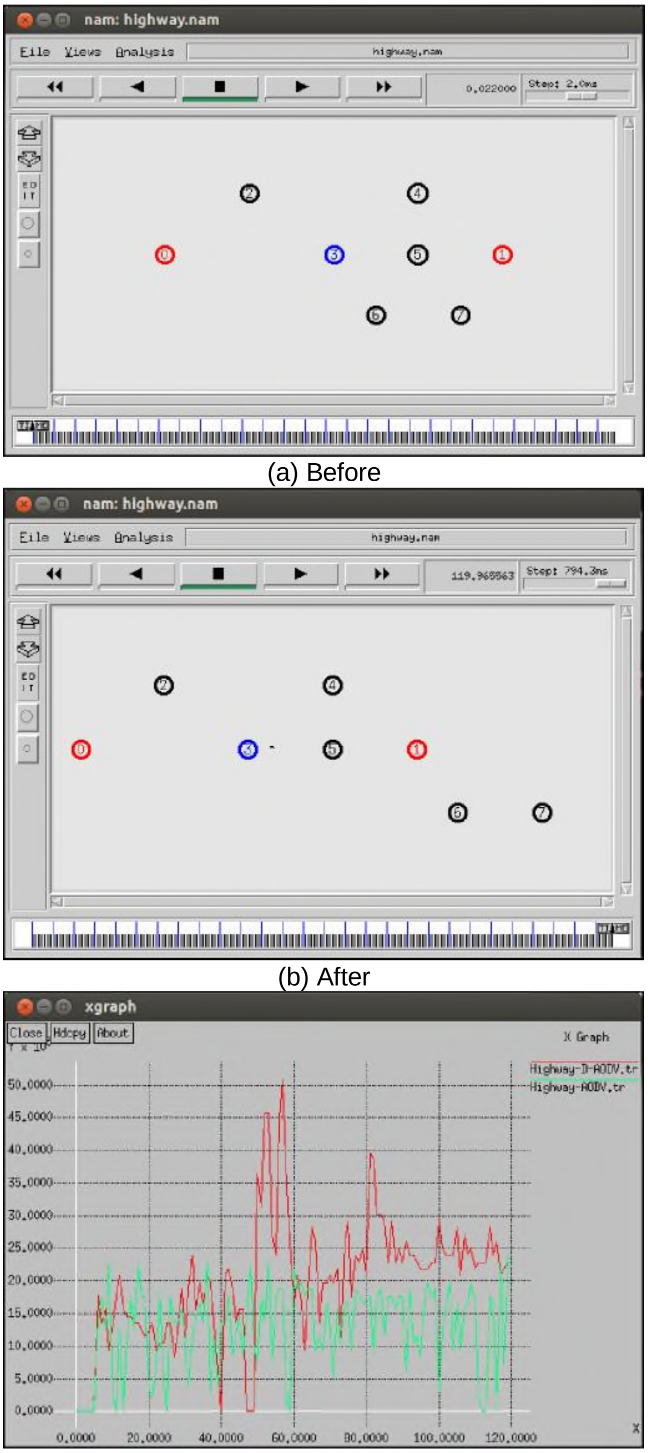
In the AODV, because the source node transfers 2,975 messages to the destination node 1, and the destination node 1 receives 1,479, the message reception rate becomes 49.71%. But, in the AODV, if the experimental time exceeds 55 seconds, the destination node 1 can receive messages no more. Considering the experimental time, the message reception rate of the MPTDC is a little better.

Table 5. The Number of Messages that each Node Receives

	MPTDC		AODV	
Send	node0	3,284	node1	2,975
	node3	12,240		
	node4	756		
	Total	16,280	Total	2,975
Received	node3	6,112	node 3	1,479
	node4	367		
	Total	6,479	Total	1,479
Rate (%)	39.80		49.71	

4.1.2 In case of DCT=1 (in a Highway)

In the experiment of message propagation in a Highway, 8 nodes were deployed in Figure 13(a), the node 0 was set as a source node and the node 1 as a destination node. Besides, the simulation had been done for 120 seconds, the node 0, 2, 3, 4, 5, 1 were moved in the left direction, and the node 6, 7 in the right direction. The Figure 13(b) shows the result that the nodes were moved. In the experiment, the node 0, 2, 3 are the same members belonging to the same cluster, the node3(cluster header) receives the messages that the node 0 and 2 transferred, and the node 3 transfers the received messages to the node 1.



(a) Before

(b) After

(c) The number of propagated message

Figure 13. Message Propagation in a Highway

Figure 13(c) shows the number of propagating messages. In this Figure, 50 seconds elapsing, because the MPTDC transfers the messages that the node 3 received to the node 1 along the paths generated by the node 4, 5, 6 and 7, the number of propagating messages is increased.

The propagation technique proposed in this paper is generally stable in message transmission, compared to the existing AODV. Table 6 shows the number of messages that the MPTDC and the AODV propagates and receives.

Table 6. The Comparison of the Number of Messages

	MPTDC		AODV	
Send	node3	4,458	node1	3,472
	node6	2,692		
	Total	7,150	Total	3,472
Received	node3	2,228	node 4	688
			node 5	807
	node6	2,309	node 7	12
	Total	4,537	Total	1,507
Rate (%)	63.45		43.40	

In the MPTDC, because the node 3(cluster head) belonging to the source node 0 transfers the message to the destination node 1, the node propagating messages becomes the node 3 and 6. At this time, the node 3 and 6 each transfers 4,458 and 2,692 messages to the destination node 1.

In the MPTDC, the destination node each receives 2,228 and 2,309 messages from the node 3. Therefore, the message reception rate is 63.45% and if the message integrity transferred from the node 3 and 6 is verified, message reception rate is 96.49%.

By contrast, in the AODV the source node0 transfers 3,472 messages to the destination node1 and the destination node1 each receives 688, 807 and 12 messages from the node4, 5 and 7. Therefore, the message reception rate is 43.40% and if the message integrity transferred from the node 4 and 5 is verified, message reception rate is 85.25%.

Considering the experimental result, the message reception rate of the MPTDC is improved.

4.1.3 In Case of DCT=2 (in an Urban Intersection)

In the experiment of message propagation in an Urban Intersection, 9 RSUs and 25 nodes were deployed in Figure 14.

When nodes are distributed like Figure 14 and the source node4 transfer messages to the destination node5, the shortest path is node4→node24→node5. But because the node24 and 5 are beyond the scope of propagation and no path can be established, in the case of Figure 14 the path on which messages can practically be transferred is as follows.

Path A: node4→node9→node10→node3→node11→node12→node13→node0
→ node14→node15→node1→node19→node20→node21→node2→node25
→ node26→node27→node5

Path B: node4→node18→node17→node16→node1→node19→node20→node21
→ node2→node25→node26→node27→node5

Path C: ndoe4→node22→node23→node7→node29→node32→node8→node33
→ node28→node5

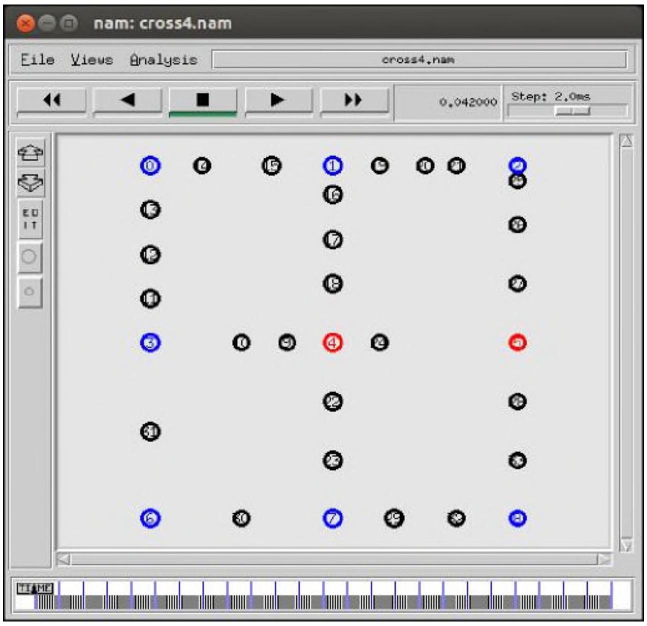


Figure 14. Message Propagation in an Urban Intersection

The AODV transfers messages by using the Path C with the smallest number of hops, but the MPTDC transfers them by using Path B which has the smaller number of hops than Path A and is greater than Path C in density. The result is shown in Figure 15. Figure 15 shows that the AODV stops transferring messages between 20 and 30 seconds, and between 105 and 120 seconds, the MPTDC transfers them stably. That is, because it establishes the message propagation path by considering density and reduces disconnection, messages are transferred stably.

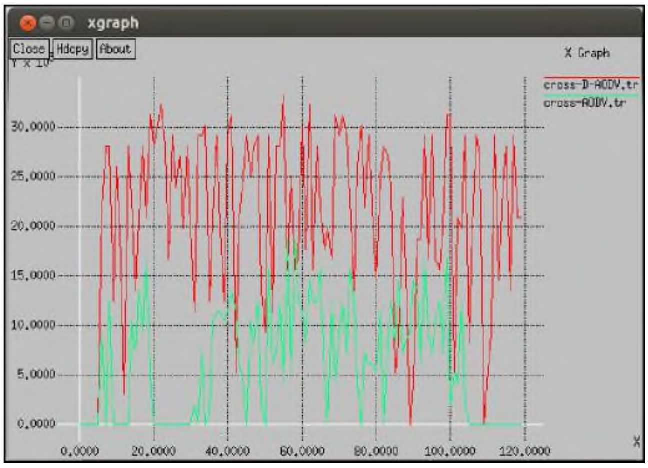


Figure 15. The Number of Propagated Messages

In the simulation, the source node 4 had transferred messages to the destination node 5 for 120 seconds. Figure 16 shows the number of messages that the destination node5 received. The node 5 received 9,428 messages through Path A, 9,628 through Path B and 9,187 through Path C.

Therefore, if the MPTDC decides the Path B as the optimal path, the messages can be transferred accurately and rapidly.

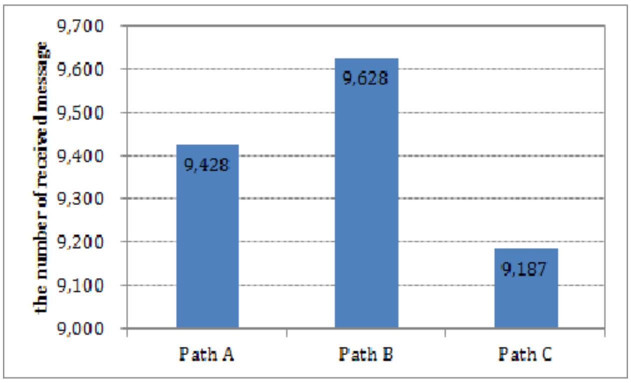


Figure 16. The Result of Message Propagation

4.2 Security Estimation

The Cluster Key proposed in this paper not only detects an Sybil attack by verifying whether each vehicle is the member of each cluster but also supports safe communication from the message forgery and the message tampering by verifying the signature generated by a Cluster Key.

The TI and ATI proposed in this paper have each timestamp. The MPTDC confirms the valid time of messages by the timestamp and deletes it after the TI and ATI go out of a critical time. Due to it, the MPTDC can prevent a Replay attack.

5. Conclusion

VANET service supports a safe service like inter-vehicle information transmission, collision protection, emergency alert, road condition alert, etc through the gathering and providing of real time traffic information.

This paper classifies roads on the basis of density and proposes the message propagation technique suitable for the classification. Therefore, this paper has good efficiency as follows. First, the MPTDC generated a Cluster Key to ensure an identity between vehicles.

Second, the MPTDC detects a Sybil attack to use ID by stealth by ensuring an identity between vehicles with a Cluster Key.

Third, the MPTDC improves the communication efficiency of VANET by aggregating frequently occurring redundant messages.

Fourth, the MPTDC reduces traffic accidents because drivers drive safely with the high reliability by message integrity.

Fifth, the MPTDC transfers traffic information to a destination accurately by selecting the path of message propagation with density.

Acknowledgements

This research was supported by Basic Science Research Program though the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A2062415).

References

[1]. K.-Y. Cho, H.-S. Nam and S.-C. Kim, “Multicast Routing Protocol for VANET Environments using FER”, Journal of Computer Science and Engineering: Information Networking, vol. 40, no. 2, **(2013).**

[2]. PRESERVE (PREpearing SEcuRe VEhicle to X Communication Systems) Deliverable 1.1, Security Requirements of Vehicle Security Architecture, **(2011).**

[3]. S.-W. Lee and B.-G. Lee, “Vehicle Communication Security Technology Trends”, National IT Industry Promotion Agency, vol. 1556, **(2012).**

[4]. S. B. Lee, G. Pan, J. Park, M. Gerla and S. Lu, “Secure incentives for commercial ad dissemination in vehicular networks”, Proceeding of the 8th ACM international symposium on Mobile ad hoc networking and computing, **(2007).**

[5]. S. B. Lee, J. Park, M. Gerla and S. Lu, “Secure Incentives for Commercial Ad Dissemination in Vehicular Networks”, IEEE Transactions on Vehicular Technology, vol. 61, no. 6, **(2012).**

[6]. H. Hartenstein and K. P. Laberteaux, “A tutorial survey on vehicular ad hoc networks”, IEEE Communication magazine, vol. 46, no. 6, **(2008).**

[7]. Y. Toor, P. Muhlethaler and A. Laouiti, “Vehicle ad hoc networks: applications and related technical issues”, IEEE communications surveys & tutorials, vol. 10, no. 3, **(2008).**

[8]. H.-T. Wu and W.-S. Hsieh, “RSU-based message authentication for vehicular ad-hoc networks”, Multimedia Tools and Applications, vol. 66, **(2013)**.

[9]. A. Aijaz, B. Bochow, D. Florian, A. Festag, M. Gerlach, R. Kroh and L. Tim, “Attacks on inter vehicle communication systems-an analysis”, Proceeding of the 3rd WIT, **(2006).**

[10]. K. Plossl, T. Nowey and C. Mletzko, “Towards a security architecture for vehicular ad hoc networks”, Proceeding of the 1st International Conference on Availability, Reliability and Security (ARES 2006), **(2006),** Vienna, Austria.

[11]. J. Y. Choi, M. Jakobsson and S. Wetzel, “Balancing Auditability and Privacy in Vehicular Networks”, Proceeding of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks (Q2SWinet ’05), **(2005).**

[12]. J-P. Hubaux, S. Capkun and J. Luo, “The security and privacy of smart vehicles”, IEEE Secur Priv., vol. 2, no. 3, **(2004).**

[13]. G. Kounga, T. Walter and S. Lachmund, “Proving reliability of anonymous information in VANETs”, IEEE Transactions on Vehicular Technology, vol. 58, no. 6, **(2009).**

[14]. X. Lin, X. Sun, P-H. Ho and X. Shen, “GSIS: a secure and privacy preserving protocol for vehicular communications”, IEEE Transactions on Vehicular Technology, vol. 56, no. 6, **(2007).**

[15]. X. Lin, X. Sun, X. Wang, C. Zhang, P-H. Ho and X. Shen, “TSVC: timed efficient and secure vehicular communications with privacy preserving”, IEEE Transactions Wireless Communication, vol. 7, no. 12, **(2008).**

[16]. R. Lu, X. Lin, H. Zhu, P-H. Ho and X. Shen, “ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications”, Proceeding of the IEEE INFOCOM 2008, **(2008),** Phoenix, AZ, USA.

[17]. M. Raya and J-P. Hubaux, “The security of vehicular ad hoc networks”, Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN ’05), **(2005),** Alexandria, VA, USA.

[18]. C. Zhang, R. Lu, X. Lin, P-H. Ho and X. Shen, “An efficient message authentication scheme for vehicular communications”, IEEE Transactions on Vehicular Technology, vol. 57, no. 6, **(2008).**

[19]. C. Zhang, R. Lu, X. Lin, P-H. Ho and X. Shen, “An efficient identity-based batch verification scheme for vehicular sensor networks”, Proceeding of the IEEE INFOCOM 2008, **(2008),** Phoenix, AZ, USA.

[20]. A. Fujii, G. Ohtake, G. Hanaoka and K. Ogawa, “Anonymous authentication scheme for subscription services”, Proceedings of the 11th International Conference, KES 2007 and XV. Italian Workshop on Neural Network Conference on Knowledge-Based Intelligent Information and Engineering Systems: Part III, LNCS, vol. 4694, **(2007)**.

[21]. Y. Sun, Z. Feng, Q. Hu and J. Su, “An efficient distributed key management scheme for group-signature based anonymous authentication in VANET”, Security Communication Networks, vol. 5, no. 1, **(2012).**

[22]. S. Zhang, J. Tao and Y. Yuan, “Anonymous authentication oriented vehicular privacy protection technology research in VANET”, In International Conference on Electrical and Control Engineering (ICECE), **(2011).**

[23]. H. Zhu, T. Liu, G. Wei and H. Li, “PPAS: privacy protection authentication scheme for VANET”, Cluster Computing, vol. 16, no. 4, **(2013).**

[24]. D. Cham and E. V. Heyst, “Group signatures”, Proceedings of 1991 advances in cryptology- EUROCRYPT, **(1991).**

[25]. D. Boneh, X. Boyen and H. Shacham, “Short group signatures”, Advances in Cryptology-CRYPTO 2004, LNCS 3152, **(2004).**

[26]. A. Shamir, “Identity-based cryptosystems and signature schemes”, Proceedings of 1984 advances in Cryptology Crypto, Springer, **(1984),** New York, USA.

[27]. F. Wang, Y. J. Xu, L. Wu, D. Liu and L. H. Zhu, “Authenticating and tracing biological anonym of VANET based on KMC decentralization and two-factor”, Proceeding of the 11th annual international conference on mobile systems, applications, and services (MobiSys ’13), ACM, **(2013),** New York, USA.

[28]. L. Zhang, Q. Wu, A. Solanas and F. J. Domingo, “A scalable robust authentication protocol for secure vehicular communications”, IEEE Transactions on Vehicular Technology, vol. 59, no. 1, **(2010).**

[29]. M. Wang, D. Liu, L. Zhu, Y. Xu and F. Wang, “LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication”, Computing, Springer, **(2014)** March 25.

[30]. L. Wischhof, A. Ebner, H. Rohling, M. Lott and R. Halfmann, “SOTIS - A self-organizing traffic information system”, Proceeding of the 57th IEEE vehicular technology conference, **(2003).**

[31]. T. Nadeem, S. Dashtinezhad, C. Liao and L. Iftode, “TrafficView: Traffic data dissemination using car-to-car communication”, ACM SIGMOBILE Mobile Computing and Communication Review, vol. 8, no. 3, **(2004).**

[32]. R. Kumar and M. Dave, “A Framework for Handling Local Broadcast Storm using Probabilistic Data Aggregation in VANET”, Wireless Personal Communication, vol. 72, no. 1, **(2013).**

[33]. Q. Sun and H. Garcia-Monica, “Using Ad-hoc Inter-Vehicle Networks for Regional Alerts. Technical Report”, Stanford University, **(2004),** http://infolab.stanford.edu/~qsun/ research/alert.pdf.

[34]. J. Zhao and G. Gao, “VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks”, IEEE Transactions on Vehicular Technology, vol. 57, no. 3, **(2008).**

[35]. S. U. Rahman and U. Hengartner, “Secure Crash Reporting in Vehicular Ad hoc Networks”, Proceeding of the 3rd International Conference on Securing and Privacy in Communication Networks (SecureComm’2007), **(2007).**

Authors

ByungKwan Lee (First Author)

He received his B.S. degree from Pusan National University in 1979, the M.S. degree in Computer Science from Chung-Ang University in 1986 and the Ph.D. degree in Computer Science from Chung-Ang University in 1990 in Korea. He has been a professor of Computer Science at Catholic Kwandong University in Korea since 1988. He was a visiting professor at Saginaw Valley State university, Michigan, USA during 2000~2001. He is a permanent member of the KISS and KIPS

EunHee Jeong (Corresponding Author)

She received her B.S. degree from Kangnung National University in 1991, the M.S. degree in Computer Science from Kwan-Dong University in 1998 and the Ph.D. degree in Computer Science from Kwandong University in 2003 in Korea. She has been a professor of department of Regional Economics at Kangwon National University in Korea since 2003, Sept. She is a regular member of the KSII. Her current research interests are Sensor Network, IT security, web programming, and e-commerce.

YiNa Jeong

YiNa Jeong received her B.Eng. degree from Kwandong National University in 2011, the M.Eng. degree in Computer Science from Kwan-Dong University in 2012. She is currently working towards a doctorate in Computer Science from Catholic Kwandong University. Her current research interests are Sensor Network, IT security, and Network security.