J Inf Process Syst, Vol.10, No.1, pp.103~118, March 2014
http://dx.doi.org/10.3745/JIPS.2014.10.1.103

pISSN 1976-913X
eISSN 2092-805X

Cooperation-Aware VANET Clouds: Providing Secure Cloud Services to Vehicular Ad Hoc Networks

Rasheed Hussain* and Heekuck Oh*

Abstract—Over the last couple of years, traditional VANET (Vehicular Ad Hoc NETwork) evolved into VANET-based clouds. From the VANET standpoint, applications became richer by virtue of the boom in automotive telematics and infotainment technologies. Nevertheless, the research community and industries are concerned about the under-utilization of rich computation, communication, and storage resources in middle and high-end vehicles. This phenomenon became the driving force for the birth of VANET-based clouds. In this paper, we envision a novel application layer of VANET-based clouds based on the cooperation of the moving cars on the road, called CaaS (Cooperation as a Service). CaaS is divided into TIaaS (Traffic Information as a Service), WaaS (Warning as a Service), and IfaaS (Infotainment as a Service). Note, however, that this work focuses only on TIaaS and WaaS. TIaaS provides vehicular nodes, more precisely subscribers, with the fine-grained traffic information constructed by CDM (Cloud Decision Module) as a result of the cooperation of the vehicles on the roads in the form of mobility vectors. On the other hand, WaaS provides subscribers with potential warning messages in case of hazard situations on the road. Communication between the cloud infrastructure and the vehicles is done through GTs (Gateway Terminals), whereas GTs are physically realized through RSUs (Road-Side Units) and vehicles with 4G Internet access. These GTs forward the coarse-grained cooperation from vehicles to cloud and fine-grained traffic information and warnings from cloud to vehicles (subscribers) in a secure, privacy-aware fashion. In our proposed scheme, privacy is conditionally preserved wherein the location and the identity of the cooperators are preserved by leveraging the modified location-based encryption and, in case of any dispute, the node is subject to revocation. To the best of our knowledge, our proposed scheme is the first effort to offshore the extended traffic view construction function and warning messages dissemination function to the cloud.

Keywords—VANET Clouds, Security, Privacy, Traffic Information, Data Dissemination, Cloud Computing

※ This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Ministry of Education, Science and Technology (No. 2012-R1A2A2A01046986).
※ This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2012-R1A1A2009152).
※ This research was supported by the MSIP (Ministry of Science, ICT & Future Planning, Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2013-H0301-13-1002) supervised by the NIPA (National IT Industry Promotion Agency).
Manuscript received April 29, 2013; first revision June 18, 2013; accepted August 25, 2013.
Corresponding Author: Heekuck Oh (hkoh@hanyang.ac.kr)
* Dept. of Computer Science and Engineering, Hanyang University, ERICA Campus Ansan, 426-791, Korea (rasheed@hanyang.ac.kr, hkoh@hanyang.ac.kr)

Copyright ⓒ 2014 KIPS

1. INTRODUCTION

VANET (Vehicular Ad Hoc NETwork) has evolved from MANET (Mobile Ad Hoc NETwork) as its specialized breed by employing vehicles as nodes where the mobility of the nodes is restricted by the road topology. VANET has gone through ample amount of research to provide drivers and consumers with safe, reliable, and infotainment-rich driving experience. Nevertheless, automobile companies are still reluctant to deploy VANET in full scale due to security and privacy challenges [1]. Since VANET is directly related to human lives, security and privacy issues are of paramount importance and have been addressed for a considerably long time by the academia and industry [2-4]. There have been unbelievable advancements in technology, and vehicles moving on the road cannot be considered merely mechanical and used for driving from source to destination. They are envisioned to provide more reliable, safer, and infotainment-rich driving experience to consumers as well. In the very near past, a number of VANET researchers argued that future high-end vehicles will under-utilize their resources because such vehicles will be computation-rich, processing-rich, communication-rich, and storage-rich. Then, considering a vehicle only for traveling from source to destination might be equivalent to wasting its aforementioned resources somehow. Thus, Olariu *et al.* came up with a new paradigm shift from traditional VANET to VANET clouds [5-6]. In VANET clouds, vehicular nodes leverage and/or pool their resources and use/form cloud resources as well. There are three basic architectures of VANET-based clouds in literature: VC (Vehicular Clouds), VuC (Vehicles using Clouds), and HVC (Hybrid Vehicular Clouds) [7].

1.1 Design Rationale

The driving force behind VANET-based clouds is the emergence of CC (Cloud Computing) because CC has changed the way people think about establishing a firm or a company for instance, which needs a considerable amount of upfront money and man-work [8]. The slogan of cloud computing is, "*why would you buy anything when you can rent it*?" With cloud computing, it is possible for consumers and service providers to have virtually everything available for rent, which can save them a reasonable amount of upfront money and establishment cost. In the same way, the aforementioned resource-rich vehicles can tap their resources to form on-demand cloud or to use the available cloud resources for different services in VANET. The reasons for offshoring the traffic information dissemination and warning message dissemination function to the cloud are as follows: the effective transmission range is a serious issue in VANET, and recent research studies show that the transmission range may become phenomenally degraded in the presence of obstacles (tall vehicles, vegetation, and buildings) [22,23]. In such scenarios, cloud infrastructure may be ideal provided that a high-speed and consistent gateway connection is present to connect in a timely manner with clouds. Thus, vehicles could crowd-source their coarse-grained information to get the fine-grained one from the cloud. Besides, due to the advancements in telecommunication systems, automobile manufacturers nowadays are outfitting their cars with 4G Internet connections.

1.2 Contributions

The contributions of this paper are as follows:

a. We consider the VuC framework proposed by Hussain *et al.* [7] and define another

application layer atop the vehicular cloud computing stack and name it CaaS (Cooperation as a Service). The main function of this layer is to enable VANET and CC to cooperate with each other in the form of information and service exchange. This layer is further divided into three sub-layers: TIaaS (Traffic Information as a Service), WaaS (Warning as a Service), and IfaaS (Infotainment as a Service).

b. We propose a novel service called TIaaS, which provides the vehicular nodes with fine-grained traffic information based on their current and near-future locations and their heading. This service is realized through the constant high-frequency cooperation between vehicles on the road and the cloud through either static or mobile gateways.

c. We also propose another service called WaaS, which provides the vehicles with timely warning messages in case of any hazard situation (for instance, ambulance approaching, black ice on the road, deadly accident, or traffic jam) along with the necessary security measures that must be taken by the vehicles in AoI (Area of Interest). IfaaS is concerned with entertainment delivery to the vehicles through cloud services and is put off for future work.

d. Due to the stringent security and privacy requirements in VANET and its successor, vehicular clouds, we leverage a secure, modified version of location-based encryption to provide location security and privacy, without which the security of the cooperators (vehicles) would be at stake and movement profiles could be generated.

e. We ensure conditional anonymity in our proposed scheme, wherein the privacy of the nodes is preserved as long as they are benign. In case of any dispute, our proposed scheme lets the revocation authorities revoke the node[1] by using back-track information in the messages.

f. Our scheme includes a new variation of V2C (Vehicles to Cloud) communication paradigm for cooperation and service exchange. Vehicles share their current coarse-grained whereabouts information in the form of beacons with each other and with static/dynamic road-side units, which then forward the information to the cloud. Similarly, cloud provides vehicles with services. Nevertheless, we focus on the traffic information and warnings.

The rest of the paper is organized as follows: Section 2 outlines the state of the art regarding VANET and VANET clouds; In Section 3, we outline the VANET-based cloud, which serves as baseline for our proposed scheme; Section 4 discusses our proposed scheme; The evaluation of our proposed scheme is outlined in Section 5; The conclusions and future directions are presented in Section 6.

2. State of The Art regarding VANET and VANET-based Clouds

There has been a considerable amount of research on VANET for the past couple of decades from the applications, architecture, design, and security standpoint [2-4, 9-10]. Kargl *et al.* [1] discussed implementation, performance, and research challenges in VANET in detail. Similarly, Papadimatroits *et al.* [11] outlined design and architectural issues in VANET. In other words,

[1] We use the terms 'node', 'vehicle' and 'vehicular node' interchangeably throughout the rest of the paper.

most of the research work on VANET is carried out from the security and privacy standpoint because those are the main obstacles in VANET deployment. Privacy requirements have been discussed in great detail by Dotzer *et al.* in [12]. Privacy-enhancing solutions and data-centric misbehavior solutions can be found in [9, 10, 13].

The services offered by VANET are not limited to safety warnings and non-safety applications like traffic congestion and routing information but also include value-added services such as high-speed tolling, mobile infotainment, Internet-on-the-move, movies-on-demand, and IPTV [14].

With the rate of advancements in technologies, computation, communication, and storage resources are virtually becoming unlimited. This dream has been made a reality by cloud computing wherein the notion of "*pay-as-you-go*" has been put forth. People do not have to pay for huge upfront money to establish their firms; instead, they can get all they want -- for rent. Still, the main question remains: is cloud computing here to stay, or will it flop like many other technologies [15]? Current market players in the field of CC include Google, Amazon, and Microsoft. Nevertheless, security and privacy hiccups are alike in both VANET and cloud computing. Storage security is another hot issue in cloud computing these days. Bessani *et al.* [16] proposed a scheme to remedy the storage security problem in cloud computing through encryption, encoding, and replication of data on diverse clouds, which led to a cloud-of-clouds. Cachin *et al.* [17] conducted a comprehensive survey on data integrity and consistency in clouds and discussed recent research trends in cryptography and distributed computing by addressing the aforementioned security primitives.

Olariu *et al.* were the first group to envision the combination of VANET and cloud computing [5-6]. They proposed AVC (Autonomous Vehicular Clouds) offering potential applications to VANET users. The authors also discussed briefly the research challenges in vehicular clouds. Abuelela *et al.* [6] suggested taking conventional VANETs into the cloud and envisioned that, in the future, the under-utilized VANET resources could be utilized by combining VANET with cloud computing [5]. Taking a step ahead, Bernstein *et al.* [18] proposed a Platform as a Service (PaaS) model for the mobile vehicular domain with possible potential applications. Yan *et al.* [19] outlined the security and privacy challenges in vehicular clouds. They discussed the challenges associated with the features of vehicular clouds, e.g., authentication of high-mobile vehicles and complexity of trust relationships among multi-players caused by intermittent short-range communication.

Hussain *et al.* took a step further and put forward the taxonomy of VANET-based clouds into three large architectural frameworks: VC, VuC, and HVC [7]. Recently, Qin *et al.* proposed a cloud-based routing scheme in VANET named VehiCloud, which provides routing services for VANET [20]. Vehicles share their current and future location information in the form of waypoints with clouds; the cloud then provides them with optimal routing information. The limitation of their proposed scheme is that the future location of the vehicle depends on the current velocity and behavior of the driver.

We put forth the idea of CaaS wherein vehicular nodes and cloud infrastructure cooperate with each other to provide VANET users with services such as traffic information, timely warning messages, and infotainment. Traffic information is provided to subscriber vehicles as a service. Vehicles share their coarse-grained traffic information in the form of MV (Mobility

Fig. 1. VANET using Clouds (VuC) Framework [7]

Vector)[2], and cloud then processes the coarse-grained information collected from a number of vehicles to construct fine-grained traffic information and forward it to the vehicles based on their current and future locations. Similarly, timely warnings are sent to the vehicles based on their current locations in a timely manner in case of hazard situations (for instance, traffic jam on the road, black ice on the road, etc.).

3. VANET-Based Clouds

Hussain *et al*. [7] recently proposed the architectural framework for VANET-based clouds. Specifically, they proposed three kinds of frameworks for VANET-based clouds: VC, VuC, and HVC. In the case of VC, vehicles moving on the road pool their resources to form a mobile cloud for certain purposes. For instance, to schedule dynamically the traffic lights in a considerably large area, interested vehicles in the vicinity pool their resources and form the cloud [5]. Broker(s) are selected among the vehicles to manage the cloud. After completing the task, the authorized entities release the pooled resources. Note that the vehicular nodes serve as service providers in this paradigm. In this paper, we deal only with the VuC framework. The general form of VuC is shown in Fig. 1.

Fig. 1 shows the VuC framework wherein VANET users use cloud services while on the move. To use cloud services, along with other considerations, there must be available, reliable, and high-speed connection between vehicles and cloud modules. This connection serves as the only way for vehicles to be able to use the cloud services. The entity connecting vehicles to the cloud is referred to as GT (Gateway Terminal), and it provides the virtualization property. Physically, this virtualization layer consists of two entities: static GTs and mobile GTs. Static GTs are realized through RSUs (Road-side Units), and mobile GTs, through mobile vehicles with 4G Internet access capability. Services offered by VuC include CAA (Cooperative

[2] Without loss of generality and ease of understanding, we use the terms mobility(movement) vectors and beacons interchangeably throught the rest of the paper.

Awareness Applications), real-time traffic information, warning messages, and infotainment. From the VANET application standpoint, CAA is of prime importance. Keeping in mind the size and frequency of data generation in CAA, VuC would be the ideal framework for providing services to VANET.

Fig. 2. CaaS (Cooperation as a Service) Taxonomy

4. Proposed CaaS (Cooperation as a Service)

In this section, we outline our proposed CaaS scheme for vehicular clouds. The main theme of our proposed scheme is illustrated in Fig. 2. CaaS is divided into three services: TIaaS, WaaS, and IfaaS. The vehicles share their coarse-grained traffic information with the cloud infrastructure, and the cloud decision module intelligently provides the vehicles with current fine-grained traffic information and potential warning messages in case of any hazard situation on the road.

The main difference between traffic information and warning dissemination through traditional multi-hop communication and through cloud infrastructure is that: 1) The traditional multi-hop communication paradigm can be affected by the blind spots issue that arises from the Non Line-of-Sight (NLoS) problem, whereas Cloud infrastructure alleviates the aforementioned problem [22,23]. 2) Virtually all roads are covered by the cloud infrastructure. This argument partially holds because of the fact that, in normal scenarios, vehicular nodes will likely be on every road segment, thereby enabling cloud infrastructure to have cooperation from all road segments. On the other hand, in case of traditional VANET, to cover the road segments, assumptions are made on the dense deployment of RSUs. 3) To extend the traffic view from single-hop (short range) to long range, multi-hop communication is essential in normal scenarios; due to the reliability and coverage issues of multi-hop wireless communication, however, it may not favor the ephemeral VANET. Moreover rebroadcasting including its variations is another problem. On the other hand, in the cloud-based approach, these concerns are taken to the upper level, and cloud covers almost every road segment.

Table 1. Outlines the notations that will be used throughout this paper.

Table 1. Notations

No.	Notation	Explanation
1	GT_i	*i*-th Gateway Terminal
2	VID	Vehicle ID
3	ZID	Zone ID
4	SID	Segment ID
5	$TD_{x,t}$	Traffic Density at segment x at time t
6	K_V	Vehicle's individual secret key
7	K_Z	Zone-level common secret key
8	$K_{geolock}$	Geolock-based encryption key
9	$h()$	Collision-resistant hash function
10	$h(m,k)$	Keyed HMAC on message m with key k
11	MV_i	*i*-th movement vector
12	$Data$	Mobility data in the movement vector
13	M_{TI}	Traffic information message

4.1 Requirements

The proposed scheme must fulfill the following requirements:

a. *Anonymous Cooperation*: The vehicles must cooperate with the cloud infrastructure in anonymous fashion wherein messages must not be linked to specific users.
b. *Avoid Profilation and provide Location Confidentiality*: The cooperation between vehicles and cloud infrastructure must not let the adversary generate movement profiles against specific users, and their location information must remain confidential.
c. *Conditional Privacy*: Due to the conflict between liability and privacy requirements, middle-way, conditional privacy must be preserved. In case of any dispute, the vehicle in question must be revoked by the revocation authorities.
d. *Non-Frameability*: Benign vehicles must not be framed as a result of message replay, forging, etc.
e. *Seamless coverage of NLoS*: Because of vegetation, buildings, pedestrians, and tall vehicles, the line of sight is considerably affected, thereby affecting the effective transmission range of vehicles. The proposed scheme must deliver the traffic information to vehicles even in case of NLoS.

4.2 Network Model

Our network model is illustrated in Fig. 3. We divide our network into two architectures connected by a virtualization layer, which consists of GT. The first architecture is VANET,

which consists of vehicular nodes on the road serving both as producers (they produce information to the clouds) and consumers (they subscribe to traffic information and warning messages from the clouds) at the same time. The cloud architecture mainly consists of Authenticator, CCP (Cloud Collecting Point), CKB (Cloud Knowledge Base), and CDM (Cloud Decision Module). The authenticator is responsible for handling subscriptions from vehicles and authenticating them. The data-contained MVs are collected at CCP and sent to CKB for processing, and CDM decides which vehicles must receive which fine-grained data. It is worth noting that the RSUs (Roadside Units) and some vehicular nodes with 3G/4G support act as terminal gateways to the cloud denoted by GT. Subscriber vehicular nodes have access to cloud through these terminal gateways. VANET is physically divided into small zones depending on the physical conditions like traffic density in the region and population, whereas zones are further divided into small manageable segments to deliver the right information and/or warning to the vehicles. The main idea of CaaS is depicted in Fig. 3.

Fig. 3. Proposed Network Model of Cooperation as a Service in VANET Clouds

Fig. 3. illustrates the network model for our proposed scheme. The network virtualization layer works as mediator between VANET and cloud infrastructure, realized through RSUs (Road-Side Units). It also serves as Communication Bridge between the two infrastructures wherein the virtualization layer takes cooperation as input from VANET to the cloud infrastructure and outputs different services from cloud to VANET infrastructure. In our case, the cooperation is in the form of coarse-grained information that is processed and refined at the cloud and delivered to VANET users (subscribers).

4.3 Location-based Encryption

Location-based encryption refers to an encryption scheme wherein the receiver of the encrypted message must be physically present at the location defined by the sender of the

message. More precisely, location information is used to generate the key used for encryption and decryption. The purpose of location-based encryption is twofold: to ensure location confidentiality against outsiders and to keep insiders from manipulating the contents of the message. For the notions of outsiders and insiders, refer to [2].

Traditionally, in VANET, beacon messages are sent in plaintext. Such scenario gives room for outsiders to generate movement profiles of the targets. Outsiders could also manipulate the location information to create illusions and subsequently launch Sybil attacks. It is somehow essential to ensure location confidentiality against outsiders. Note, however, that insiders are still a risk since they have access to -- and can manipulate -- the location information. To decrease the effect of manipulation, we propose an extended version of Yan *et al.*'s location-based encryption [21]. Their scheme uses only GPS information to construct the geolock, but we argue that GPS information is publicly available, and their scheme depends on the assumption that GPS information is private. Our proposed geolock-based encryption is given in Fig. 4.

Fig. 4 shows the construction process of geolock key denoted by $K_{geolock}$, which is used to encrypt MV. The Geolock key construction module takes as input the effective region size, message lifetime (date & time), and zone-level secret key K_Z shared among the zone members, and then multiplexes and scrambles these values altogether to calculate the hash value from the scrambled content. The effective region size is used to define the physical region where $K_{geolock}$ is effective. Message lifetime defines the validity period of the message, which helps prevent the useless lingering around of a stale message in the network. K_Z is distributed among the vehicles of each zone beforehand, and vehicles moving from one zone to another are required to change their K_Z accordingly. The receiving vehicles must be physically present in a certain geographic region at a certain time; they must have the descrambling function and must hold a valid K_Z specified by the sender to decrypt the message encrypted with $K_{geolock}$. The main reason for using geolock-based encryption is to ensure location confidentiality against outsiders, remedy message contents manipulation, and prevent outdated messages from lingering around the network.

Fig. 4. Geolock-based Encryption: Construction of $K_{geolock}$

4.4 Traffic Information as a Service (TIaaS)

4.4.1 Secure Mobility Vectors (MV)

According to the DSRC standard, every vehicle in VANET broadcasts beacon messages with a predefined frequency containing whereabouts information that includes position, speed, and heading information leveraged by VANET application to construct traffic views for drivers. These traffic views enable drivers to make timely decisions in case of hazard situations like traffic jam ahead or icy road. For security reasons, we encrypt the message with $K_{geolock}$, which has already been discussed. We assume that the information from clouds to VANET is secure, and that it uses a fast backbone channel. Then, from GT to subscribers, location-based encryption is used to encrypt the fine-grained information. Only physically present subscribers can have access to the fine-grained traffic information because we use zone-key K_Z in location-based encryption. Another realization of using location-based encryption is that the cloud module sends fine-grained traffic information to the subscribers based on their current location and the direction of their movement. Encrypting message with $K_{geolock}$ ensures that only the concerned subscribers at the PoI (Point of Interest) get the traffic information. The format of MV is given below.

$$MV_i = \left(Data, h(Data, K_Z), h(K_V)\right)_{K_{geolock}} \tag{1}$$

$$Data = (h(VID), t_{cur}, loc_{cur}, vel_{cur}, dir)$$

t_{cur} is the current time and loc_{cur}, vel_{cur}, and dir are the current location, current velocity, and direction of movement, respectively. It is worth noting that mobile GTs are chosen among the vehicular nodes with rich communication resources (4G Internet); thus providing an extra communication channel to reach static GTs. When an encrypted MV reaches GT, GT at first decrypts MV with the current $K_{geolock}$, and then saves $h(VID)$ and $h(K_V)$ in its database for liability reasons. These two parameters will be able to help RAs (Revocation Authorities) in revocation if there is a dispute. GT then sends MV to the cloud through a secure channel.

4.4.2 Fine-grained Traffic Information Dissemination

It is an active service for the vehicles (more precisely the subscribers) wherein fine-grained traffic information and warnings are delivered to the subscribers based on their current physical and near-future locations. VANET is divided into physical domains, with each domain having its own potential cloud architecture for traffic information dissemination. To guarantee the delivery of the right information to subscribers, the domain is further divided into small manageable zones, and each zone has its own zone-level common key K_Z that is used to construct $K_{geolock}$. Going down to another level of hierarchy, the fine-grained information is further divided into segments because the subscribers may only have a certain area of concern; this logically means that vehicles want to know the traffic conditions ahead of them. At the segment level, they can be provided with the best relevant traffic information. The fine-grained traffic information message M_{TI} is given below.

$$M_{TI} = \left(ZID, SID, TD, AV, LD, others, h(contents)\right)_{K_{geolock}} \tag{2}$$

Where ZID and SID refer to the zone number and segment number, respectively, and correspond to a physical location under consideration. TD denotes the traffic density, AV means the average velocity of the vehicles in that segment, and LD refers to the lane density of vehicles in segment number SID. The $others$ in the traffic information message means the warning message in case of any hazard situation in the segment under consideration, e.g., traffic congestion notification, road construction, etc. The $contents$ represent the aforementioned contents of message M_{TI}.

4.5 Warning as a Service (WaaS)

In the previous section, we discussed TIaaS in VANET-based clouds environment. In case of any hazard situation on the road -- for instance, fog, or icy road -- the driver must have a timely warning message in hand to make the right decision to avoid deadly accidents before it is too late. CDM in cloud infrastructure has twofold advantages: it produces fine-grained traffic information from coarse-grained mobility vectors, and it monitors the traffic conditions and patterns in each segment(s) and zone. In case of any deviation from the normal behavior, in addition to normal fine-grained traffic information, it also sends the appropriate warning message to the vehicles in that particular segment. The dangerous conditions and their respective warning types could be saved in CDM beforehand. CDM calculates the average traffic density using the formula below. Note that, to calculate traffic density with only movement vectors in hand, we can do so by recording movement vectors for a particular time duration $\Delta t = t_i - t_{i-1}$, and then divide the number of movement vectors by the frequency of the movement vectors. We calculate the average traffic density from the j number of individual traffic densities.

$$TD_{SID,avg} = \frac{\sum_{t=1}^{j} TD_j}{j} + \epsilon \tag{3}$$

And

$$TD_{SID,\Delta t} = \frac{\sum_{i=t_k}^{t_{k+1}} MV_i}{f_{MV}} + \omega \tag{4}$$

Where $TD_{SID,avg}$ denotes the average traffic density at segment SID and $TD_{SID,\Delta t}$ means the traffic density in segment SID at a particular time duration Δt. f_{MV} is the frequency of the movement vector messages. ϵ and ω are the error margins caused by packet drop problems in wireless communications, which will likely happen. To compensate for the loss and error margin in traffic density calculation, we included the aforementioned parameters. It is worth noting that the aforesaid traffic density calculation mechanism is privacy-aware wherein no identification information is used. CDM calculates vehicular traffic density from only mobility vectors in hand. Nevertheless, we assume that there might be other means to carry out this function as well. The same mechanism is also used for for velocity. When CDM encounters deviation from normal traffic behavior, it includes a warning in the traffic information as well in addition to fine-grained traffic information. In other words, for instance, for the smooth functioning of VANET, the following conditions must be met:

$$TD_{SID,avg} < TD_{SID,max} \; and \; Vel_{SID,avg} < \alpha \tag{5}$$

Where $TD_{SID,avg}$ is the average traffic density in segment SID and $TD_{SID,max}$ denotes the maximum allowed traffic density in segment SID. Depending on the size of the segment, dimensions of individual vehicles, number of lanes on the road, and inter-vehicular distance, the maximum traffic density can be calculated in a certain segment. If the average traffic density exceeds the threshold, then CDM sends traffic jam warning messages to the following vehicles to change their routes or slow down, whichever seems appropriate for the driver or decision-making module of the car safety system. Similarly, $Vel_{SID,avg}$ denotes the average velocity of the vehicles in segment SID, and α is the minimum threshold velocity in SID. If the velocity is less than the threshold, then CDM can trigger a traffic jam warning to the following vehicles. The aforementioned process is illustrated in the algorithm below. The algorithm takes MV from GTs as input and stores it in the knowledge base of the cloud and extracts data from MV, followed by constructing fine-grained data corresponding to each road segments and sending over to the corresponding GT, which then forwards it to the subscribers. This process is done over a specified time interval.

Algorithm: Fine-grained cooperation dissemination

1. Procedure: FGCDissemination (Fine-Grained Cooperation Dissemination)
2. Input: $b_{i,\Delta t} \in B_{\Delta t}, \Delta t = [t_i, t_j]$
3. Output: $(TI, W)_{[t_i,t_j]}$, (Deliver fine-grained traffic information and warnings about time duration Δt.)
4. $\{b_1, b_2, \ldots, b_k\} \in B_{seg_i}$ Extract beacons of different segments.
5. **For** each $Seg_i \in Zone_i$
6. Extract information from the beacon (location, speed, heading, etc.) and store it in the respective segment buffer.
7. Construct TI and W corresponding to every segment in every zone $Seg_i \in Zone_i$.
8. **End For;**
9. Send $(TI \; and \; W)_{Seg_i,\Delta t}$ to Seg_i, (Send traffic information and warning messages corresponding to each segment Seg_i.)

5. EVALUATION

In this section, we evaluate our proposed scheme. The security requirements in our proposed scheme are *message authentication*, *message integrity*, *confidentiality*, *timeliness*, *privacy protection*, *anonymity revocability*, and *non-frameability*. The security of both MV and M_{TI} is guaranteed in our proposed scheme. First of all, the messages are sent in encrypted form, thereby guaranteeing confidentiality. Nevertheless, the level of security depends on the underlying security algorithm used. Moreover the vehicles or T_i , both of which do not hold valid K_Z, cannot construct $K_{geolock}$. $K_{geolock}$ keeps outsiders from manipulating the messages and also limits the effect of stale messages in the network; when the validity period expires, then the current $K_{geolock}$ cannot be constructed. Moreover, $K_{geolock}$ updates itself in a very robust manner. The integrity of the contents is checked by $h(Data, K_Z)$. Due to the high frequency of MV (in order of milliseconds), we use loose authentication for MV by using keyed HMAC. Thus, our proposed scheme fulfills authentication and message integrity in case of MV. We analyze our proposed scheme with the help of the following lemmas:

Lemma 5.1*: The proposed scheme makes it hard to impersonate another benign node.*

Proof: The mobility data is encrypted with $K_{geolock}$, and the message itself contains hash values calculated with K_Z and hash of the original secret key. To impersonate another vehicle, the adversary must do the following: obtain the current K_Z and construct $K_{geolock}$. From another angle, the time duration required to construct $K_{geolock}$ is short; therefore, the adversary must be present physically in the effective region of $K_{geolock}$. Moreover, in case of K_Z compromise, only the current zone will be affected. If K_Z is not compromised, then it will be very hard for the adversary to impersonate another vehicle. ■

Lemma 5.2: *The proposed scheme preserves conditional anonymity wherein, in case of any dispute, the nodes are subject to revocation.*

Proof: The messages do not contain any identity information in plain text that could be used by the adversary to link the message to the sender. In other words, if the adversary collects a set of messages, it is hard to link the messages to the same sender. Moreover, MV and M_{TI} are exchanged anonymously. Meanwhile, revocation authorities are still able to revoke a user and/or a node in case of any dispute. Since GT_i saves the values $h(VID)$ and $h(K_V)$ in a table, in case of any dispute, GT_i can provide the values in question to RAs, which have already saved the vehicle's secret key information to their database beforehand. By looking up the hash table, the revocation complexity can be as good as $O(1)$ depending on the hash function and its implementation. ■

Lemma 5.3: *The vehicles' credentials as examined and saved by GTs and Cloud do not pose any threat to user privacy.*

Proof: Since messages are exchanged between cloud infrastructure and vehicles on the road through GTs, GTs must decrypt the incoming messages destined for cloud with $K_{geolock}$, and then save the two parameters $h(VID)$ and $h(K_V)$ for liability issues. The security of these two parameters is dependent on the security of the underlying hash function used. If we assume that the underlying hash function is secure enough, then we can argue that the exposure of these two hash values to GTs and cloud infrastructure poses no threat to the privacy of the node because hash values would not give any clue as to the real identity of the vehicle. ■

The size of zones is an important parameter for limiting the effect of keys compromise. Keeping in mind the role of zone key in the construction of $K_{geolock}$, the smaller the size of the zone is, the smaller will be the effect of the K_Z compromise. Conversely, smaller zone size means smaller anonymity set for vehicles, thereby reducing the anonymity. Thus, the size of the zone must be a tradeoff between anonymity and affected set of users in case of K_Z compromise.

We now analyze our proposed scheme from the perspective of the computational overhead incurred by our proposed scheme. To the best of our knowledge, the best relevant work to our proposed scheme is that by Qin *et al*. [20] and that by Bernstein *et al*. [18]. Our scheme is the

extension of Hussain *et al*.'s VuC [9], and we introduce cooperation between VANET and cloud computing. Qin *et al*. leverages TSLG (Time Space Link Graph) for defining vertices and edges in VANET. In their proposed scheme, every vehicle can be source and destination at the same time. Thus, in the worst case, the number of links can be $\mathrm{n}(\mathrm{n}-1)/4$ on the average, and the order of routing optimization is $\mathrm{O}(\mathrm{n}^2)$ where n is the number of vehicles in the network.

Like Qin *et al*., Bernstein *et al*. do not address security concerns in PaaS (Platform as a Service) architecture in connected cars. The computation overhead incurred by our proposed scheme, when sending cooperation data to Cloud infrastructure, is $2H + 1E$ operations wherein H denotes hashing operation and E refers to encryption. In the case of M_{TI}, CDM performs $1H + 1E$ operations.

6. CONCLUSIONS

In this paper, we put forth CaaS (Cooperation as a Service) architecture for VANET clouds. CaaS is divided into three sub-architectures :TIaaS (Traffic Information as a Service), WaaS (Warning as a Service), and IfaaS (Infotainment as a Service). Highly mobile vehicular nodes share their coarse-grained MVs (Mobility Vectors) with cloud infrastructure through the stationary or mobile GTs (Gateway Terminals). Cloud, after processing and constructing fine-grained traffic information and warning messages based on the physical segments of the road, sends it back to the subscriber vehicles through GTs in the respective road segments. The proposed scheme preserves conditional privacy and other security parameters such as authentication, integrity, and non-frameability. Moreover, the proposed scheme is significant from a number of perspectives including NLoS (Non Line-of-Sight) issues, effective transmission range, and construction of extended traffic view. The current solutions suffer from the aforementioned issues due to lack of LoS, height of vehicles, and obstacles parameters in the simulation tools. Besides, cloud is known to offer unlimited resources that could be used in virtually every domain. Additionally, the data generated from vehicles (for instance, according to the DSRC standard, beacons are generated in order of milliseconds) can be referred to as big data with respect to the computing power of the individual vehicles. By using cloud resources, the data can be processed efficiently according to the desired results, i.e., fine-grained information from individual coarse-grained mobility vectors. In the future, we plan to look more into the subscribing process of the vehicles and incentive-based TIaaS and WaaS.

REFERENCES

[1] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T. Ta-Vinh, G. Calandriello, A. Held, A. Kung, and J.P. Hubaux, "Secure vehicular communication systems: implementation, performance, and research challenges," *Communications Magazine, IEEE*, vol. 46, no. 11, 2008, pp.110-118.

[2] M. Raya and J.P. Hubaux, "Securing vehicular Ad Hoc networks," *Journal of Computer Security*, vol. 15, no. 1, 2007, pp.39-68.

[3] T. Leinmuller, E. Schoch, and C. Maihofer, "Security requirements and solution concepts in vehicular ad hoc networks," *Proceeding of Wireless on Demand Network Systems and Services, 2007. WONS '07. Fourth Annual Conference on*, 2007, pp.84-91.

[4] D. Antolino Rivas, J.M. Barceló-Ordinas, M. Guerrero Zapata, and J.D. Morillo-Pozo, "Security on

VANETs: privacy, misbehaving nodes, false information, and secure data aggregation," *Journal of Network and Computer Applications*, vol. 34, no. 6, 2011, pp.1942-1955.

[5] S. Olariu, M. Eltoweissy, and M. Younis, "Towards autonomous vehicular clouds," *ICST Transactions on Mobile Communications and Applications*, vol. 11, no. 7-9, 2011, pp. 1-11.

[6] M. Abuelela and S. Olariu, "Taking VANET to the clouds," Book Taking VANET to the Clouds, Series Taking VANET to the clouds, ed., Editor ed.^eds., ACM, 2010, pp.6-13.

[7] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, "Rethinking vehicular communications: merging VANET with cloud computing," *Proceedings of IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom'12)*, pp.606-609, 2012.

[8] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, 2010, pp.50-58.

[9] R. Hussain, S. Kim, and H. Oh, "Towards privacy-aware pseudonymless strategy for avoiding profile generation in VANET," *Information Security Applications Lecture Notes in Computer Science* 5932, H. Youm and M. Yung, eds., Springer Berlin / Heidelberg, 2009, pp.268-280.

[10] R. Hussain, S. Kim, and H. Oh, "Privacy-aware VANET security: putting data-centric misbehavior and Sybil attack detection schemes into practice," *Information Security Applications Lecture Notes in Computer Science* 7690, D.H. Lee and M. Yung, eds., Springer Berlin / Heidelberg, 2012, pp.296-311.

[11] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. D. Ma, F. Kargl, A. Kung, and J. P. Hubaux, "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, pp.100-109, Nov 2008.

[12] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in *Privacy Enhancing Technologies*. vol. 3856, G. Danezis and D. Martin, Eds., ed: Springer Berlin Heidelberg, 2006, pp.197-209.

[13] F. Scheuer, K. Posse, and H. Federrath, "Preventing profile generation in vehicular networks," Proceedings of Networking and Communications, 2008. WIMOB '08. IEEE International Conference on Wireless and Mobile Computing, 2008, pp. 520-525.

[14] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications*, vol. 31, pp. 2803-2814, 2008.

[15] T. W. Wlodarczyk and R. Chunming, "An initial survey on integration and application of cloud computing to high performance computing," *Proceedings of Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on*, 2011, pp. 612-617.

[16] A. Bessani, M. Correia, B. Quaresma, F. Andrese, and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds," presented at the *Proceedings of the Sixth Conference on Computer Systems*, Salzburg, Austria, 2011.

[17] C. Cachin, I. Keidar, and A. Shraer, "Trusting the cloud," *SIGACT News*, vol. 40, pp. 81-86, 2009.

[18] D. Bernstein, N. Vidovic, and S. Modi, "A cloud PAAS for high scale, function, and velocity mobile applications - with reference application as the fully connected car," *Proceedings of Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on*, 2010, pp. 117-123.

[19] G. Yan, D.B. Rawat, and B.B. Bista, "Towards secure vehicular clouds," Proceedings of Complex, Intelligent, and Software Intensive Systems (CISIS), 2012 Sixth International Conference on, 2012, pp. 370-375.

[20] Y. Qin, D. Huang, and X. Zhang, "VehiCloud: Cloud computing facilitating routing in vehicular networks," *Proceedings of the IEEE 11th International Conference on Trust, Security, and Privacy in Computing and Communications*, pp. 1438-1445, 2012.

[21] Y. Gongjun, S. Olariu, and M. Weigle, "Providing location security in vehicular Ad Hoc networks," *Wireless Communications, IEEE*, vol. 16, pp. 48-55, 2009.

[22] R. Meireles, M. Boban, P. Steenkiste, O. Tonguz, and J. Barros, "Experimental study on the impact of vehicular obstructions in VANETs," *Proceedings of the IEEE Vehicular Networking Conference (VNC),* 2010, pp. 351-358.

[23] M. Boban, R. Meireles, J. Barros, P. Steenkiste, and O. K. Tonguz, "TVR- Tall Vehicle Relaying in Vehicular Networks," [Online], http://arxiv.org/pdf/1212.0616v1.pdf.

Rasheed Hussain

He received his B.S. in Computer Software Engineering from N-W.F.P University of Engineering and Technology, Peshawar, Pakistan in 2007 and M.S. degree in Computer Engineering from Hanyang University, South Korea in 2010. Currently he is working toward the Ph.D. degree in Computer Engineering from Hanyang University, South Korea. His main research interests include information security and privacy issues in VANET (Vehicular Ad Hoc NETworks), information dissemination in VANET, VANET applications, cloud computing, and VANET-based clouds. He is currently working on emergent VANET-based clouds. He has published several papers on VANET-based clouds and has been actively involved in framework design, mitigating security challenges in VANET-based clouds, and introducing new services through VANET-based clouds.

Heekuck Oh

He received his B.S. degree in Electronics Engineering from Hanyang University in 1983. He received his M.S. and Ph.D. degrees in Computer Science from Iowa State University in 1989 and 1992, respectively. In 1994, he joined the faculty of the Department of Computer Science and Engineering, Hanyang University, ERICA campus, where he is currently a professor. His current research interests include network security and cryptography. Prof. Oh is the president of Korea Institute of Information Security & Cryptology, and is a member of Advisory Committee for Digital Investigation in Supreme Prosecutors' Office of the Republic of Korea. He is also a member of Advisory Committee for Internet Security under Korea Communications Commission. He is the corresponding author of this paper.