UNIVERSITY OF NIS FACULTY OF MECHANICAL ENGINEERING

THE SIXTH INTERNATIONAL CONFERENCE
TRANSPORT AND LOGISTICS

til
2017

VEHICULAR CLOUD: CHALLENGES AND OPPORTUNITIES

Branka MIKAVICA[1]
Aleksandra KOSTIĆ-LJUBISAVLJEVIĆ[1]
Vesna RADONJIĆ ĐOGATOVIĆ[1]

[1)]University of Belgrade Faculty of Transport and Traffic Engineering

Abstract

Vehicles represent an increasingly valuable source of computing and sensing resources. These resources may be harnessed with a conventional cloud computing systemsin a common platform, vehicular cloud network. It is a new hybrid techonology that has a meaningful impact on traffic management and road safety. In this paper we observe deployment possibilities of vehicular cloud networks as an important segment of Intelligent Transportation Systems (ITS). An analysis of challenges and opportunities of vehicular cloud networks is presented.

Keywords*: vehicles, cloud computing, ITS*

1 INTRODUCTION

Vehicular Ad Hoc Networks (VANET) are considered as one of the crucial elements of the ITS due to increasing number of the vehicles distributed around the world. One of the primary goals of ITS is to provide innovative applications and services related to traffic management. The next generation of vehicles is characterized by possibility of gathering information from the environment, as well as sharing those information with adjacent vehicles and Road Side Units (RSU). However, each vehicle has limited computation and storage resources due to the requirements of small size and low-cost hardware systems. Emerging applications, including in-vehicle multimedia entertainment, vehicular social networking and location-based services, require complex computation and large storage. Therefore, an individual vehicle cannot provide an efficient support for these applications. A very promising solution is to share the resources among or nearby vehicles, thus creating a temporary cloud. Network efficiency can be significantly improved by merging conventional clouds and these temporary clouds. In order to utilize the excessive on-board resources in the transportation system along with the latest computing resource management in conventional clouds, the concept of the Vehicular CloudNetworks (VCN) has appeared, as a prominent step forward for ITS [1, 2]. It provides significant benefits to the whole transportation system, as well as the drivers, passengers and pedestrians. Main difference between vehicular and conventional clouds is distributed ownership and hence, the unpredictable availability of computational resources. Due to high traffic mobility, the vehicular cloud systems are built on dynamic physical resources. Therefore, it experiences inherent challenges which increase complexity of its implementation.

This paper is organized as follows. After the introductory remarks, fundamentals od vehicular cloud networking are presented in the Section 2. Architecureand necessary operations in these systems are also described in this Section. Section 3 presents advantages and possible applications of vehicular cloud networks. Challenges and open issues in vehicular cloud networking are analyzed in Section 4. Concluding remarks are given in Section 5.

2 FUNDAMENTALS OF VEHUCULAR CLOUD NETWORKING

In order to support high bandwidth demanding applications with complex computation, the cooperation between vehicles and adjacent RSU is needed. Computational and storage resources are shared among them which results in a temporary cloud with more resources. Network efficiency can be further enhanced by merging conventional clouds with temporary clouds. Temporary clouds are convenient for applications such as traffic management, safety applications and sharing information about traffic conditions. Conventional clouds may offer complex applications such as providing in-vehicle entertainment to the vehicular user.These resources operate as a common virtual platform. Each vehicle incorporated in the vehicular cloud has three categories of resources: data storage, sensors and computing [3]. Contents generated from vehicle applications, sensors and conventional multimedia files are stored into data storage. It enables data sharing among cloud members. Sensors can detect events in the vicinity of the vehicle. External systems can read the sensor data and may have the possibility to control the sensor. Computing resources in the vehicle are limited and represent a collection of mobile resources. The architecture and operations in VCN are explained below.

1.1. VCN Architecture

The architecture of VCN in proposed in [4]. It consists of three levels: vehicular cloud, VC, infrastructure cloud, IC, and back-end-cloud, BEC, as shown in Fig. 1.

Physical resources of vehicle in vehicular cloud, i.e. storage and computation, are shared between only a group of vehicles. In general, vehicular network consists of vehicles with both high and low mobility. Therefore, several possible contexts arise. Mobility of the vehicles in urban areas is reasonably low in comparison with mobility in highways. Cooperation among vehicles is possible for a longer period of time so formation and existence of vehicular clouds in urban areas enable provisioning of different applications such as video surveillance of public transport. In rural areas, vehicles collaborate for a very short period of time. Therefore, vehicular cloud has short life cycle. In addition, vehicular cloud implementation is even more difficult due to low frequencies of vehicles appearance. The best possible scenario for vehicular cloud implementation is parking lot. Mobility of the vehicles is negligible. The life cycle of vehicular cloud is significantly longer in comparison with rural and urban areas. The computation and storage resources of parked vehicles can be used to form vehicular cloud covering particular location.

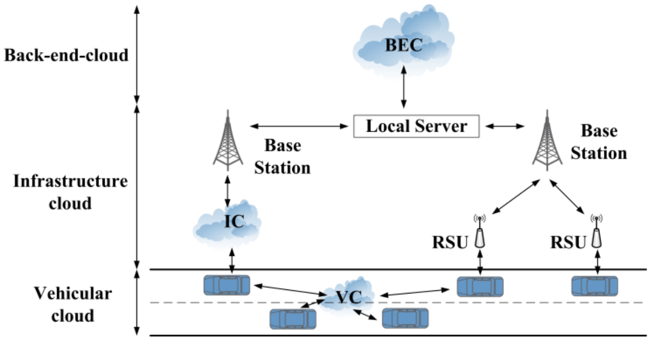

Fig. 1 Vehicular cloud network archritecture

Infrastructure clouds are mostly initiated by adjacent RSU along the road. Vehicles on the road require the access to the services provided by cloud. IC provide small geographical coverage around RSU location [5]. Communication between various infrastructure clouds is performed through dedicated local servers. Considering that both static and mobile entities in this constellation are involved in IC, technical complexity of IC development varies for different scenarios of vehicular networks. Urban areas are characterized by vehicles of relatively low mobility and excessive adjacent infrastructure. Therefore, the implementation and existence of IC is enabled due to the availability of numerous RSU. Various applications are supported by IC in urban areas, such as remote navigation and traffic management. IC deployment in rural areas is constrained due to lack of adjacent infrastructure and high mobility of vehicles. In this scenario, only temporary cloud can be formed between RSU and vehicle in short time period. When vehicles have negligible mobility and adjacent infrastructure is available (parking lot scenario), the implementation of IC in the vicinity of certain RSU is achievable. Combination of VC and IC results in high efficiency and better network performances.

Back-end-cloud refers to the largest conventional cloud in vehicular environment. This cloud owns resources that can be used by vehicles for extensive data storage and computation [6]. BEC supports provisioning of high bandwidth demanding applications, such as in-vehicle multimedia.

1.2. VCN Operations

For given collection of resources from vehicles and RSUs and their potential interconnections, VCN system performs certain operations in order to establish a virtual computing platform. When a vehicle runs an application, it takes role of a cloud leader and has possibility to recruit new cloud members that provide their resources in order to form a vehicular cloud for the application. The types and search range of required resources depend on given application. Search range may be a predefined distance, a road section or an intersection [3]. Therefore, cloud leader is responsible for cloud initiation in a vehicular network. The role of cloud leader may have vehicle or adjacent RSU. Vehicular cloud is established in the scenario where cloud leader is a vehicle and no adjacent RSU participate in cloud formation. If the request for cloud initiation belongs to the RSU and surrounding vehicles respond to that request, the resulting cloud is infrastructure cloud.

Cloud leader invites vehicles and adjacent RSUs in its vicinity by transmitting resource request messages (RREQs) in order to create a cloud. Member intending to share its resources responds to the cloud leader with resource reply message (RREPs) [3].After notifying RREPs, the cloud leader selects cloud members and organizes a cloud. The selection process may tend to minimize total resource usage in the cloud along with the correct operation of the application.Cloud leader is also in charge for members' IDmaintenance and assignment of different tasks and application. The application is distributed to the cloud members depending on the availability and accessibility of their resources.Cloud members regularly communicate with cloud leader. Members can share contents based on the cloud leader permission. Maintenance of the cloud is responsibility of the cloud leader. Cloud members can dismiss membership in the cloud by requiring the resource leaving message to cloud leader. In that case, cloud leader confirms the release and selects a replacement among members that initially sent RREPs in the resource discovery phase. New member should have enough resources to complete the task assigned to the leaving member. Cloud leader distributes given task to the new cloud member and updates the network topology information. When cloud leader moves out of the cloud range, it broadcasts the cloud release message and releases the resources so that the other cloud members can reuse them.

3 POSSIBLE APPLICATIONS OF VCN

Different vehicles and RSU share their resources along with the conventional BEC thus enabling a wide range of potential applications. VCN supports video surveillance in urban areas. It enables tracking vehicles or people using high definition (HD) video to ensure security. Considering that HD video in real time requires large storage, vehicular clouds are promising solution.

Vehicular clouds enable managing applications depending on their bandwidth requirements in order to provide better spectrum allocation. Applications with small bandwidth requirements such as vehicle safety and warning applications can be used directly through VC, while high bandwidth demanding applications such as vehicular user multimedia can be processed via IC and BEC.Resources within vehicle may not be sufficient for accurate 3D geographic maps maintenance. Hence, vehicular cloud resources may support real time vehicular navigation.Another important application of vehicular cloud networks is remote traffic management. In the situation of long queue of vehicles on the highway, information may be shared via vehicular clouds. Vehicular cloud is observing the segment of traffic congestion by transferring the time, coordinates and final destination to a navigation server through on-board vehicle navigators. The navigator server in BEC determinates the optimal routes by constructing traffic load map and the traffic pattern matrix, estimates road segment loads and delays and returns optimized routes to the vehicles [8].

Traffic signals define the signal cycle length and the green phase lengths. Optimization of signal system is performing offline at the isolated intersection or at the corridor lever. The time periods are set by the timing plans for certain time periods, for instance - weekend mornings or afternoon peak hours. This method has several disadvantages. It requires accurate historical data of traffic flows in order to ensure that the signal timing plans are convenient for given traffic volume conditions. In addition, this method is not adjustable to uncertain changes in traffic conditions. Hence, vehicular clouds can enhance the signal system performances by making dynamic use of a vehicular network [2].

Vehicular networks may support evacuation managing. Transportation agencies often develop simulations in order to identify possible traffic control strategies for potential evacuation events. In these situations, vehicular clouds can provide information about travel time calculations, availability of resources such as food, water, gasoline etc. The vehicles involved in the evacuation procedure form vehicular cloud which cooperates with emergency rescue response office.

Nowadays vehicles are equipped by sensing devices for efficient and safe operation. For instance, cameras can help driver to stay in the lane by tracking the lines on the road. Vehicles query the sensors of the other vehicles in close vicinity in order to obtain a valuation of a potential road accident ahead, road conditions, potential holes on the road etc. Therefore, vehicular cloud can be formed dynamically with a large wireless sensor network.

4 CHALLENGES AND OPEN ISSUES IN VCN

Several issues and challenges related to vehicular clouds need to be appropriately addressed. Security and privacy aspects are of crucial importance. These aspects are more complex in comparison with conventional networks due to high mobility of cloud members, dynamical characteristics of the environment, heterogeneity of the vehicles and frequent network topology changes. In addition, establishing trust relationships among cloud members presents a vital part of trustworthy communication which is necessary in this context. Cloud members should have greater insight in the process of sharing information [8, 9]. Furthermore, limited storage on mobile devices, insufficient battery life, scalability and service availability are challenges in vehicular cloud computing, as well.

Vehicular cloud networks involve different assets that potentially could be exposed to the attacker. The assets are vehicles, vehicular user, wireless communication, adjacent infrastructure and clouds. In order to achieve efficient and secure vehicular cloud environment, it is necessary to consider possible threats in all assets.

In general, vehicular cloud network involve vehicles of high mobility and their communication is possible in short time period [10]. Despite that, vehicles are prone to attacks, especially on-board unit, application unit of vehicle or sensors. The possible target of the attacker may also be software running on application unit and sensors where primary goal of attacker is to introduce malware. Considering the fact that infrastructure, including RSU, is not mobile, hardware is the most vulnerable for the threats. Other threats to infrastructure include unauthorized access of attacker to software platform.

Wireless communication is a medium for data exchange between neighbouring vehicles and adjacent RSU. Possible threats in this segment is Denial of Service (DoS), tempering and alteration of the messages, creation of the congestion on wireless communication channel, etc. DoS attack can cause severe damage in the network; the attacker block the communication channel and prevents cloud members to forward important massages to the cloud, other vehicles or RSU in the vicinity. Data tempering refers to altering and modification of messages and their rerouting between vehicles, RSU and cloud [11]. Another result of DoS attack is congestion of wireless communication medium. Threats to the messages exchanged among the vehicles and adjacent RSU appear when the main interest of the attacker is to compromise message confidentiality, integrity and authenticity. Since vehicular cloud is a result of sharing of computational and storage resources of vehicles, the most vulnerable is cloud platform itself. Potential threats are the following: malware may be injected into the cloud platform, privacy may be disrupted, information of vehicular user identity, its geographical location and other sensitive information may be revealed. Infrastructure cloud includes both static and mobile entities. Hence, both cloud platform and messages propagation are exposed to the possible threats. DoS attack may prevent the static RSU to exchange messages with other members.Unauthorized members must be revealed and removed from the cloud in order to keep user information privacy.

BEC is the largest cloud in the vehicular cloud network environment and hence, it is vulnerable to various threats. The most critical among those are the data and network threats. The most severe threats in the data context are data breaches and data loss. Data breach refers to the leakage of vehicular data to an unauthorized entity. It mostly occurs due to defects in application designing, operational issues, insider attackers, and the absence of authentication, authorization and audit controls. Data loss refers to the loss of data in BEC. When vehicular data is transferred to the cloud, it will be processed by applications and stored into the cloud storage. Data loss may occur during data transfer to and from cloud, during the phase of processing by applications, or in the cloud storage [12]. If security measures are not implemented accordingly, the BEC network can be prone to different attacks. Attacker may take the credentials of cloud members in order to access their vehicular data and cloud services. This leads to loss of confidentiality, integrity and availability of vehicular data. DoS attacks may also be launched from BEC services or from outside the BEC. The consequence of these attacks is the unavailability of data, storage, computational resources and bandwidth to the legitimate cloud members.

Mobility of the nodes in vehicular cloud network topology has direct impact on the availability of computational capabilities and storage resources. In order to support fluctuating application requirements and resource accessibility on the move, appropriate related protocol architecture and networking need to be deployed. Robust and dynamic architecture is needed for aggregation of the computational and storage resources in this constellation. The system architecture should also be service-oriented and component-based with sufficient monitoring facilities in order to support reusable and extensible applications and resources.

Vehicular clouds may need the establishment of the local authority instead of central. For instance, in the situation of congestion on the road when traffic lights need to be rescheduled, the cooperation between the cloud and municipal or country authority is needed in order to achieve rapid alleviation of congestion. Therefore, the establishment of a trust management in vehicular cloud environment is useful for automated verification of actions. Effective operational policies are needed for decision support, regulation, establishing accountability metrics and standards. In the near future, it is expected that federation of different cloud will appear in vehicular cloud environment. The interoperability of different clouds, connection, synchronization, reliability and efficiency of such cloud constellations need to be properly addressed.

5 CONCLUSION

Advances in vehicular technology have provided resources such as fixed storage devices, improved computer power, cognitive radios and various types of programmable sensor nodes. These enhancements lead to improvement of safety and traffic efficiency. Vehicular cloud computing is a new technological paradigm which takes the advantages of cloud computing and merge them with VANETs. The objectives of vehicular cloud networks are the following: provisioning of computational and storage services at low cost and minimization of: traffic congestion, traffic accidents, travel time, environmental pollution and energy consumption.

When fully implemented, vehicular cloud networks can lead to meaningful enhancements in ITS in the terms of security, safety and efficiency. In a planned or unplanned evacuation or other emergency situations, vehicular cloud networks alleviate the damage to the mobile communication infrastructure. It provides a decision support system and offers a temporary replacement for the infrastructure. Extensive research is required to create a vehicular cloud network reference model, protocols and architecture for addressing evolving trust and privacy issues.

ACKNOWLEDGMENT

The paper is a part of the research done within the project No. TR 32025 from theMinistry of Education, Science and Technological Development of Serbia.

REFERENCES

1. Garai, M., Rekhis, S., Boudriga, N., 2015, *Communication as a Service for Cloud VANETs*, Proc. 20th IEEE Symposium on Computer and Communications (ISCC'15), Larnaca, Cyprus.
2. Whaiduzzaman, M., Sookhak, M., Gani, A., Buyya. R., 2014, *A Survey on Vehicular Cloud Computing*, Journal of Networks and Computer Applications, 40, pp. 325–344.
3. Lee, E., Lee, E.K., Gerla, M., Oh, S., 2014, *Vehicular Cloud Networking: Architecture and Design Principles*, IEEE Communications Magazine, 52(2), pp. 148-155.
4. Ahmad, F., Kazim, M., Adnane, A., Awad, A., 2015, *Vehicular Cloud Networks: Architecture,Applications and Security Issues*, Proc. IEEE/ACM 8th International Conference on Utility and Cloud Computing, Limassol, Cyprus.
5. Ahmad, F., Kazim, M., Adnane, A., 2015, *Vehicular Cloud Networks:Architecture and Security*, Guide to Security Assurance for Cloud Computing, Springer.
6. Yu, R., Zhang, Y., Gjessing, S., Xia, W., Yang, K., 2013, *Toward Cloud-basedVehicular Networks with Efficient Resource Management*, IEEE Network, 27(5), pp. 48-55.
7. Kim, W., Gerla, M., 2011, *NAVOPT: Navigator Assisted Vehicular routeOPTimizer*, Proc. 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Seoul, Korea.
8. Gerla, M., 2012, *Vehicular Cloud Computing*, Proc. 11th AnnualMediterranean Ad-Hoc Networking Workshop (Med-Hoc-Net), Ayia Napa, Cyprus.
9. Ronga, C., Nguyena, S.T., Jaatunb, M.G., 2013, *Beyond Lightning: A Survey on Security Challenges in Cloud Computing*, Recent Advanced Technologies and Theories for Grid and Cloud Computing and Bio-engineering, 39(1), pp. 47-54.
10. Alriyami, Q., Adnane, A., Kim Smith, A., 2014, Evaluation Criterias forTrust Management in Vehicular Ad-hoc Networks (VANETs), Proc. 3rd International Conference on Connected Vehicles & Expo (ICCVE2014), Vienna, Austria.
11. Yan, G., Rawat, D., Bista, B., 2012, *Towards Secure Vehicular Clouds*, Proc. 6th International Conference on Complex, Intelligent and SoftwareIntensive Systems (CISIS), Palermo, Italy.
12. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M., 2010, *A View of Cloud Computing*, Communications of the ACM, 53(4), pp. 50-58.

Contact address:
Branka Mikavica,
Univerzitet u Beogradu, Saobraćajni fakultet
11000 BEOGRAD
Vojvode Stepe 305
E-mail: b.mikavica@sf.bg.ac