Improving Response Time of Vehicular Ad hoc NETworks (VANET)

Qasim Zia
School of Systems and Technology
University of Management and Technology
Lahore, Pakistan
s2016114006@umt.edu.pk

Dr. Muhammad Shoaib Farooq
School of Systems and Technology
University of Management and Technology
Lahore, Pakistan
shoaib.farooq@umt.edu.pk

Dr. Adnan Abid
School of Systems and Technology
University of Management and Technology
Lahore, Pakistan
adnan.abid@umt.edu.pk

Abstract: -
Cloud Computing is a model which can be acquire through network and its objective is to despite of the place and invisibly make use of huge amount of resources related to computing. These are being leased to digital users by service providers. Because of high amount related to accidents in traffic and road user's dissatisfaction regarding response time of vehicular ad hoc networks. The main stress of current solutions is make betterment in the response time of vehicular ad hoc networks (VANET). This research aims at improving the response time by introducing the message prioritization methodology. The message with higher priority would be given resources immediately without any delay.

Keywords: VANET, cloud computing, network, message prioritization, network resources.

Introduction: -

Cloud Computing is a fresh paradigm related to computing which utilizes groups of physical resources associated with computing identified as data centers [1]. These can be arranged on request into a dynamic entity which is logical entity that can reduce and grow generally through the Internet against a rented resource fee. It provides three important digital services which are classified as Software as a Service (SaaS) (e.g. Applications), Infrastructure as a Service(IaaS) (e.g. Storage Resources), Platform as a Service (PaaS) (e.g. OS) [2]. Cloud Computing utilizes a technology which is virtualization based through which physical resources of cloud can be used to give services as a virtual or logical resource [3].

To make sure that any application that execute in cloud maintain performance, sensitivity of latency, consistency, scalability and surely security a new model was proposed recently known as fog computing in which services of computing are supplied at the cloud network edge [4].

When we discuss about vehicular networks efficiency, minimum delay, consistency and scalability are very much important but network security is something without which it is impossible to survive in this field or area [5]. It will help us enhance the safety of road and comfort of passengers Via Intelligent Transportation System(ITS). To back the mission regarding safe journey of Vehicular Ad Hoc Networks in this paper we propose the better security of Vehicular Ad Hoc Networks which extends the current security measures of Vehicular Ad Hoc Networks[6]. VANET permits computing resources which are onboard in the vehicles with the cloud computing which is traditional so that we take advantage of the vehicles abilities like storage and processing. Improved VANET security will help the drivers and other stakeholders to reduce dangerous road situations for instance finding the alternative routes, traffic lights management to reduce the congestion of roads, incidents in traffic, commercial vehicle procedures and so on [7].

Nowadays, these Intelligent Transportation System applications are given by the digital services via vehicular ad hoc networks(VANET) [8]. Therefore, VANET can be explained as the vehicles which are communicating nodes acknowledge as mobile entities which travel to a limited mobility pattern and constant entities known as roadside units (RSU) positioned at important locations for instance critical intersections, roads that are slippery, places well recognized for unsafe weather situation.

Related Work: -

VANET cloud can deliver many services of computation for reducing congestion of traffic, accidents, time related to travelling, pollution of environment etc. with minimum cost. Except this, VANET cloud can also pay attention towards vehicles that are not following traffic rules. Privacy and security are also very important creating and keeping trust between VANET cloud computing users. Many methodologies are proposed in order to fulfil the overhead requirements in the literature and they are discussed under: -

Zhu et al. [11] describe a methodology to reduce the latency of authorization related to Vehicle to Infrastructure (V2I) and the distributed revocation of public key. For purpose of authorization latency, the authors described prediction scheme which is based on mobility dependent on Multilayer Perceptron(MLP) and pattern which is infrastructure dependent Short-time Certificate Management(SCM).

Yan et al. [9][10] discuss passive and active location algorithms of security. Radar can be taken as which is very much virtual and radar which is onboard can sense the position of vehicles. Digital Signatures and Public Key Infrastructure(PKI) dependent methodologies have been well discovered in the field of VANETs. A certificate Authority (CA) produces private in addition to public keys on behalf of the actual nodes. The objective of the digital signature stands to authenticate as well as confirm the actual sender.

The objective of the encryption remains to unveil the material of the messages to the permitted receivers. Public Key Infrastructure is the methodology which is significantly structured for the purpose of security especially for the roadside setup. Yan et al described Geo Encrypt in VANETs [12]. The basic methodology adopted by them is to utilize the geographic position of the vehicle to produce the secret keys. Messages are encrypted using secret key and the text which is encoded would be transmitted to the vehicles which are receiving. The actual vehicles which are receiving must exist actually in the definite geographic area which is decided by the actual sender to become capable of message decryption.

Nowadays some concentration has been dedicated towards common security problems in cloud while not connected with vehicular network. The general answer is to minimize entree to the hardware of the cloud infrastructure. This approach can reduce risk [13].

Wang et al. declare a public key dependent authenticator which is homomorphic and the masking which is random to protect data of cloud and secure cloud data's public privacy [14]. The signatures which are aggregate of bilinear are prolonged to parallel review many users [15].

Problem Statement:

Traffic congestion exist due to variance factors like construction of road, hours of rush, and some unpredictable and unavoidable circumstances like weather, road accidents and behavior of human. The more extreme congestion is the more duration is required to eliminate.

Due to this thing there is often a case that Vehicular Ad-Hoc Network(VANET) response time increase due to large amount of request and response transactions.

Research Question: -

1. How can we decrease the response time of the Vehicular Ad-Hoc Network(VANET) so that critical vehicles like ambulance won't have to wait and have response immediately?

Proposed Framework: -

My work give stress on providing different priority messages in a vehicular Ad-hoc Network (VANET) to reduce the delay in the network during congestion. For instance, Ambulance should be given priority over the normal car because of the critical situation of the patient.

These priorities would be allocated to the message depend upon the type of the vehicles. The car would be recognized in the network as they are connected with the certification authority and Traffic Police station through Road Side Units(RSU) and built in Sensors. Moreover, the car shares its credentials with the authorities in order to recognize that car lies in which type.

Basis upon type of the car message associated with it would be given priority preference in case of congestion. So, that there would be less delay and response time would be enhanced and there would be no major loss due to delay.

Default Car Priority

Priority	Type
Pri(1)	Ambulance
Pri(2)	Government Officials
Pri(3)	Private

Future Direction: -

As future work, this research can be prolonged to control car theft, if the car is being theft by some other person, the affected person can only send a prioritized message which would be transmitted to the nearby police station. The police station would then take the necessary action and track the car using the information provided by Road Side Units(RSU).

References: -

[1] "Vital signs: Nonfatal, motor vehicle–occupant injuries (2009) and seat belt use (2008) among adults — united states," Centers for Disease Control and Prevention-US Department of Health and Human Services,1600 Clifton Rd. Atlanta, GA 30333 USA, Tech. Rep. MMWR 2011, January 2011. [Online]. Available: http://www.cdc.gov/mmwr/preview/mmwrhtml/mm5951a3.htm

[2] "Budget estimates fiscal year 2013," US Department of Transportation Federal Highway Administration, 1200 New Jersey Avenue, SE, Washington, DC 20590, Tech. Rep. FHWA FY 2013, November 2013. [Online]. Available: www.dot.gov/mission/budget/fy2013-budget estimates

[3] "Highway statistics 2012," US Department of Transportation Federal Highway Administration, 1200 New Jersey Avenue, SE, Washington, DC 20590, Tech. Rep. FI-10, October 2013. [Online]. Available: www.fhwa.dot.gov/policyinformation/statistics.cfm

[4] "The economic and societal impact of motor vehicle crashes, 2010," NHTSA, US Department of Transportation Federal Highway Administration, 1200 New Jersey Avenue, SE, Washington, DC 20590, Tech. Rep. DOT HS 812 013, May 2014. [Online]. Available: http://www.nhtsa.gov

[5] S. Olariu, I. Khalil, and M. Abuelela, "Taking vanet to clouds," Journal of Pervasive Computing and Communications, vol. 7, no. 1, pp. 7 – 21, Sep 2011.

[6] M. Eltoweissy, S. Olariu, and M. Younis, "Towards autonomous vehicular clouds," in Ad Hoc Networks, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, J. Zheng, D. Simplot-Ryl, and V. C. Leung, Eds. Springer Berlin Heidelberg, 2010, vol. 49, pp. 1–16.

[7] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, "Rethinking vehicular communications: Merging vanet with cloud computing," in Proceedings of 2012 IEEE 4th International Confernce on Cloud Computing Technology and Science, December 2012, pp. 606–609.

[8] "ns-3 tutorial," http://www.nsnam.org/docs/release/3.19/tutorial/html/index.html, 2013, [Online; accessed 09-January-2014].

[9] G. Yan, S. Olariu, and M. C.Weigle, "Providing VANET security through active position detection," *Comput. Commun.*, vol. 31, no. 12, pp. 2883–2897, Jul. 2008, Special Issue on Mobility Protocols for ITS/VANET.

[10] G. Yan, S. Olariu, and M. Weigle, "Providing location security in vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 16, no. 6, pp. 48–55, Dec. 2009.

[11] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service oriented vehicular networks," IEEE Wireless Communications, vol. 16, no. 4, pp. 16 – 22, Aug 2009.

[12] G. Yan and S. Olariu, "An efficient geographic location-based security mechanism for vehicular ad hoc networks," in *Proc. IEEE Int. Symp. TSP*,Macau SAR, China, Oct. 2009, pp. 804–809.

[13] V. G. Martinez, L. H. Encinas, and C. S. Avila, "A survey of the elliptic curve integrated encryption scheme," Journal of Computer Science and Engineering, vol. 2, no. 2, pp. 7–13, August 2010.

[14] J. Wang, T. Ma, J. Cho, and S. Lee, "Real time services for future cloud computing enabled vehicle networks," in Proceedings of Wireless Communications and Signal Processing Conference, Nov 2011, pp. 1 – 5.

[15] S. Olariu, T. Hristov, and G. Yan, The Next Paradigm Shift: From Vehicular Networks to Vehicular Clouds. Wiley-IEEE Press, 2013, ch. Mobile Ad Hoc Networking: Cutting Edge Directions, Second Edition (eds. Stefano Basagni and Marco Conti and Silvia Giordano and Andlvan Stojmenovic), pp.645–700.