www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13618-13620

Scalable and Efficient Data acquisition in Service Oriented Vehicular Adhoc Networks

[1]Nishi K.M. , [2]Indu P.

[1] M-Tech Student, Computer Science and Engineering, MES college of Engineering
Malappuram, Kerala, India
kmnishi@gmail.com

[2] Assistant Professor, Computer Science and Engineering, MES college of Engineering
Malappuram, Kerala, India
indupvimala@gmail.com

Abstract: ***Vehicular Ad Hoc Network (VANET) is the subpart of the Mobile Ad Hoc Network(MANET) that aims at enhancing the safety and efficiency of transportation systems. In VANET vehicles communicate with each other and with roadside units (RSUs). Service oriented vehicular networks are special types of VANETs that provides infrastructure based commercial services, including Internet access, real-time traffic management, video streaming, and content distribution. Many forms of attacks against service-oriented VANETs that attempt to threaten their security have emerged. The success of data acquisition and delivery systems depends on their ability to defend against the different types of security and privacy attacks that exist in service-oriented VANETs. Service-oriented vehicular security system allows VANET users to exploit RSUs in obtaining various types of data. When multiple users are connected to an RSU at a time it may results in RSU network overhead. So a scalable and an efficient system has been designed by applying certain scheduling algorithms there by avoiding Packet delay and traffic overhead.***

Keywords: RSU(Road Side Units), Security, Privacy,Scalability, Service Oriented Vehicular Adhoc Network.

1. Introduction

The development and wide utilization of wireless communication leads to the concept of intelligent communicating machines. Vehicular ad hoc network (VANET) is recognized as an important component of Intelligent Transportation Systems. VANETs are considered as an off-shoot of Mobile Ad hoc Networks (MANETs) with some distinguishing characteristics. In VANET vehicles are nodes that are dynamic and because of their high mobility and speed the network topology changes fast. On the contrary, in VANET ve-hicles move only on predetermined roads, and they do not have the problem of resource limitation in terms of data storage and power. Real time communication among vehi-cles and roadside units can help the driver to have full information on road conditions and this will enhance traffic safety and efficiency. In VANET, each vehicle is equipped with the communication devices, global positioning system and digital map that allow the drivers to communicate with each other as well as with roadside infrastructure to enhance easier and safety transportation.Each vehicle contains On-Board Units (OBUs), to communicate with each other vehicles (V2V) as well as with RSUs (V2I). VANET is a high capacity mesh network that connects the vehicles and RSUs, and the RSUs can be connected to a backbone mesh network, so that vehicles provide many other network applications and services, including Internet access to the VANET users.

Current research trends for VANETs focused on developing applications that can be grouped into the following two classes: 1) improving the safety level on the road and 2) providing infotainment application. In infotainment application RSUs are usually connected to the Internet and allow users to download maps, traffic data, and multimedia files and check emails and news. These kinds of VANETs referred to as service oriented, are expected to virtually provide all types of data to drivers and passengers. The security of VANETs is one of the most critical issues because their information transmission is propagated in open access environments. It is necessary that all transmitted data cannot be injected or changed by users who have malicious goals. Moreover, the system must be able to detect the obligation of drivers while still maintaining their privacy. There are several methods to assure security in the network world which are also applicable in wireless networks. Thus, most of protocol implementers prefer using cryptography schemes such as public key. The security of safety applications is different from the security of service-oriented applications because of their different security requirements. For example, the data exchanged in safety messages (such as location information or warnings) need not be encrypted. However, messages that contain data from infotainment applications must be tightly encrypted.

2. Related works

Many approaches have been proposed for the privacy preservation in VANET. All the systems that are proposed in the literature aims to maintain the security of data messages exchanged between users and RSUs and the location privacy of VANET users who exchange these messages. But they differ by the type of encryption scheme. J.Freudiger et al.[1]

introduced an area called Mix Zone in which several vehicles change their pseudonyms together so that an attacker will not distinguish the new pseudonym of each vehicle. Pseudonyms are randomly changing identifiers that have got a short validity period and can't be reused. K. Sampigethava et al. [2] introduced a Group concept and a Random Silent Period. In Group concept vehicles are grouped to mitigate the location tracking of any target vehicle. The group concept also provides robust anonymous access to prevent the profiling of LBS (Location based Service) applications accessed by any target vehicle. In random silent period, a join technique that enables any target vehicle to increase location privacy at opportune places during navigation, but potentially at the cost of safety and liability. Random Silent Period provides unlink ability between Locations in V2V Applications in which vehicle remains silent for a randomly chosen period. M. Raya et al. [3] introduced that message legitimacy is mandatory to protect VANETs from outsiders, as well as misbehaving insiders. Since safety messages will not contain any sensitive information, confidentiality is not required. As a result, the exchange of safety messages in a VANET needs authentication but not encryption. Therefore Digital signatures are used over other forms for message authentication. Chun-Ta Li a et al. [4] introduced a light weight Authenticated key establishment scheme to secure the communication between vehicles and roadside infrastructure in a VANET. SECSPP protocol accomplishes vehicle-to-vehicle and vehicle-to-roadside infrastructure authentication and key establishment for communication between members. It also integrates blind signature techniques into the scheme in allowing mobile vehicles to anonymously interact with the services of roadside infrastructure. Bharati Mishra et al. [5] introduced an RSU aided message Authentication scheme. It is a secure and efficient protocol for vehicular ad hoc networks that ensures both message authentication and privacy preservation. As safety related message may contain life critical information, it is a necessity that the sender as well as the message is authentic. This scheme is based on a secure elliptic curve digital signature algorithm approach that supports conditional privacy, where the user's location can be revealed at the willingness of the user. Z. Wang et al. [6] introduced a novel approach for users to start their connection in VANET in a secure way and a symmetric encryption scheme along with hierarchical password based key derivation function (PBKDF2) to strengthen the security of message to a high extent. A new handover scheme and a novel mechanism for data confidentiality have been introduced.

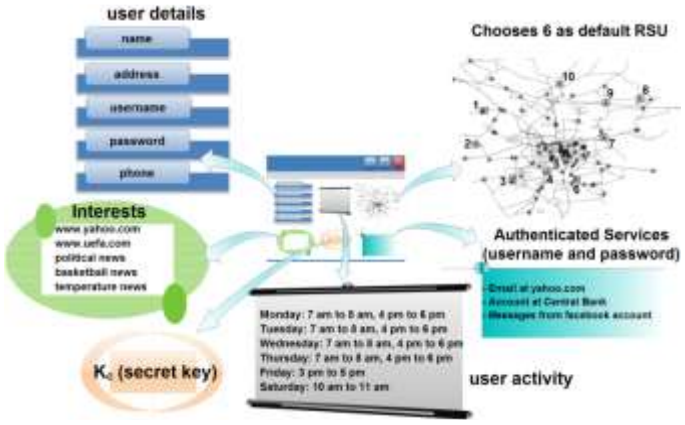
Even though this method is efficient in many ways, it has the main problem called Scalability. This system is not scalable with the increasing number of users that can connect to an RSU. The method proposed in this section 3 has effectively overcome those problems. Later in section 4 these two methods are compared on their Packet Delivery Ratio.

3. Proposed work

In this section a new and efficient mechanism that allows RSUs to make use of their free timeslots (TSs) to obtain users data and cache them until the users connect to the VANET. In our approach, an RSU estimates the periods during which a user might connect to the VANET. Also,each RSU distinguishes between the interests of different users in order not to waste its resources. It has been done by introducing an RSU scheduling mechanism to reduce the overhead in RSU network.

RSU Scheduling Mechanism

RSU builds a schedule for each day. The schedule defines the users that could connect during each TS of the day. For this schedule to be built, each user is required to submit, during registration, the times during which he expects to join the network. Figure 1, gives an example of a user registering with the RSU system in which the user should fill called user activity.



In this section, the user chooses the times which he expects to join the VANET (we refer to them from now on as periods). These times will be used by the users default RSU to build an activity profile for the user. The RSU combines the activity profiles of all users to build its schedule. The schedule of an RSU is divided into TSs which have constant values (e.g., 1 hour, 10 minutes, etc). Each RSU user registering with the RSU defines the length of its TSs according to the lengths of the periods defined by its users when they register. For example, if users define their periods as whole hours (such as Monday between 8 am and 2 pm), then the RSU sets the size of a TS to 1 hour. Each RSU builds its schedule as follows: The RSU first defines the candidate periods of each user. Then it adds these candidate periods into their corresponding TSs in the schedule and specifies for each TS its set of users. After the RSU defines the users whose data should be prepared during each TS, it redistributes the load among all TSs such that if a TS contains much load, some of the load is shifted to a directly previous TS. Hence, the RSU will prepare these interests ahead of time and caches the data until the users connect. Each piece of data could have a TTL after which it is deleted. The TSs to which the load is shifted should not be much earlier than the original TSs so that the RSU wont cache the data for a long time.

In actual scenarios, a TS could contain many users. Hence,a balancing algorithm that distributes the load evenly and keeps

the caching periods as small as possible should be applied. Round Robin Algorithm has been used as a scheduling mechanism to reduce the load .

4. Results and Analysis

The proposed system has compared with the existing one based on the parameter packet delivery ratio. Packet Delivery Ratio is the ratio of actual packet delivered to the total packet send from RSUs to users. The actual packet delivered by the RSU has increased as a result of scheduling. Figure 2 shows that Packet Delivery Ratio is considerably increased in the proposed technique.

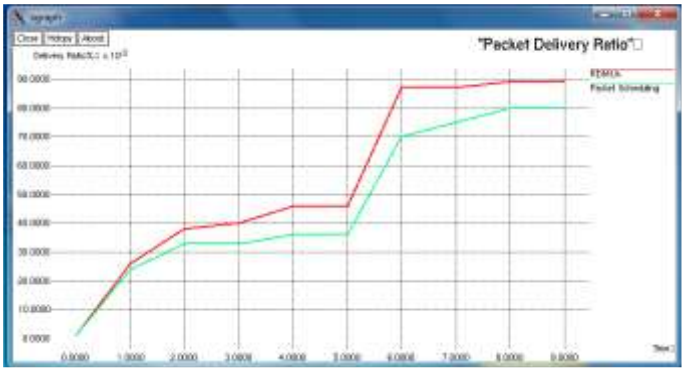


Figure 2: Packet Delivery Ratio comparison

5. Conclusion

In the Proposed system roadside units (RSUs) were exploited to satisfy the various requests of VANET users. This approach uses RSUs as delegates to acquire services from service providers without the users connecting to them. Users interests range from email messages, news, web downloading, business transactions, multimedia sharing, traffic or weather information, etc. Depending on RSUs to obtain users data puts a huge load on the RSU network and might lead to a scalability problem, especially with the large number of users. The proposed system exploits the presence of roadside units to reduce the load on vehicles and to hide the complexity of getting the required data in a secure way for them.

References

[1]J.Freudiger, M.Raya, M.Feleghhazi, P.Papadimitratos, and J.P.Hubaux, "Mix zones for location privacy in vehicular networks", Int.Workshop Wireless Netw. Intell. Transp.Syst.,Vancouver,BC,Canada,LCA-CONF-2007-016,August 2007

[2]K.Sampigethava,L.Huang,M.Li,R.Poovendran,K.Matsuura,and K.Sezaki, "AMOEBA: Robust location privacy scheme for VANET", IEEE J.Sel.Areas Commun,vol.25,Nov.2010

[3] M.Raya and J.P.Hubaux, "The security of vehicular ad hoc networks",In Proc.SASN,Alexandria,VA,pp.1121,Nov.2010

[4] Chun-Ta Li a, Min-Shiang Hwang b, Yen-Ping Chu c, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks",Elseveir,ComputerCommunications,ScienceDirect,31,2803-2814,Nov.2008

[5]Bharati Mishra,Saroj Kumar Panigrahy, "A Secure and Efficient Message Authentication Protocol with Privacy preservation", world congress on information and communication Technologies,Mumbai,India,Oct.2011

[6] Z. Wang, Y. Chen, and C. Li, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks", IEEE Trans on vehicular technology,January 2013

[7] K. Mershad and H. Artail, "SCORE: Data scheduling at roadside units in vehicle adhoc networks, in Proc. ICT, Jounieh,Lebanon, pp.16,2012