Privacy Enabled and RSU Assisted Aggregation Scheme in VANET[1)]

Rasheed Hussain*, Sangjin Kim**, Heekuck Oh*
*Dept. of Computer Science and Engineering, Hanyang University
**School of Information and Media Engineering, Korea University of Technology and Education
Email: rasheed1984@gmail.com

Abstract

In this paper, we provide a tradeoff solution to two conflicting requirements in VANET; *Privacy* and *Aggregation*. The information about traffic density is an important factor of aggregation in VANET. In our proposed scheme, densely located Road-Side Units (RSU) perform traffic density calculation and then aggregate the traffic information extracted from beacons received from the vehicles. RSUs then disseminate the aggregated traffic information to all the vehicles and neighbor RSUs. We use identityless beaconing thereby providing privacy and we do not consider the content security of beacons. We show that our scheme provides privacy in the case of aggregation, which has not been considered in previous schemes.

1. Introduction

By the virtue of Vehicular Ad-hoc Networks (VANET), in the near future it will be possible for the vehicles to communicate with each other. This will play an important role in the safe driving and early warnings in case of an emergency or dangerous situations [1] on the road. Among other security parameters like authentication, confidentiality and integrity, privacy also has par importance to these parameters [2]. In most of the research works previously done, privacy of the users and their locations have been considered in VANET. According to DSRC standard, every vehicle periodically broadcasts messages called beacons with frequency ranging from 100ms to 300ms. These beacons are used to construct a local view about the traffic conditions ahead of the vehicle. In order to avoid the de-facto standard of flooding arproach, a mechanism called aggregation is used to extend the vehicle's view about traffic conditions.i ew about tr is a long-t me trademark of sensor networks which saves both bandwidth and computut tral power.i ew about tr gives rise to new problems in the situations when beacons are is used to ooding aprivacy. In the case where beacons ooding aprivacy, it may not be possible to linkalledor more beacons to same vehicle. On the other hand,out tr is a long-t me trademark of sensoby which traffic conditions are caationsed. To caationseout tr is a long, it ico nss ired to link two or more beacons to the same vehicle because due to high frequency of beacons, it will not be possible to differentiate among beacons from same or different vehicles. But in case of privacy enabled beacons, it becomes more difficult to calculate the traffic density. For beacon's privacy, we use Hussain et al's scheme [3] which is the refined version of the Plobi's and Scheuer's scheme with symmetric cryptography and avoids any type of individual identity in the beacons. We provide the tradeoff between the privacy of beacons and aggregation. We propose two schemes regarding the tradeoff between the privacy and aggregation. Fig.2 explains the scenario.

1) "This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the HNRC(Home Network Research Center) - ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency" (NIPA-2009-C1090-0902-0035)

2. Proposed Scheme

Calculating Traffic Density:

In VANE, nodes have main concern of "how much" and not "who" about the neighbors. For privacy reasons, our beacons are sent having no identity information thereby giving no room to adversaries to make movement profiles (note that we don not consider the contents security). As aggregation of the normal beacons is used by a vehicle to extend its view about ahead traffic conditions, so traffic density is an important factor which must be included in aggregated messages. Due to our beaconing mechanism, it is not possible to s not hto s not hto t hto t hto . As a tradeoff, we enable RSU hto calculate the traffic density information and disseminate itand disthe vehicles in its under-control area. When a vehicle enters the area under certain RSU, then while sending s not,sthe vehicle gives an indication to RSU that it has entered into s noregion. This indication er ce p ccisely, is a bit ($_{snt}$) that is se-cont s not which has otly ms ning to RSU. When RSU cceives that s not,slculate increment the counter for traffic density by bn t hto . A RSU can deducte itan hto s not that a new vehicle is entered into s noregion and while exiting itan htovicinity

by an RSU, the (b_{ext}) is set in the beacon giving information to the RSU that it is no longer included in the traffic density of that particular RSU. Our beacon format is shown in fig.1. $\delta 1$ is used for revocation purpose if there is case where a vehicle must be revoked by certain authorities. Since only the sending vehicle has the individual key (K_{V_i}), so if this key is secure then no one else can calculate $\delta 1$. $\delta 2$ is used for weak authentication and it is calculated with zone key (K_Z).

Timestamp	b_{ent}	b_{ext}	G_{id}	Information	$\delta 1$	$\delta 2$

Fig. 1. Beacon Format

$\delta 1$=HMAC.K_{V_i}(T||b_{ent}||b_{ext}||G_{id}||Information) and

$\delta 2$= HMAC.K_Z(T||b_{ent}||b_{ext}||G_{id}||Information||$\delta 1$)

Aggregation:

Most of the schemes proposed for aggregation in VANET have used vehicular nodes as *Aggregators*. We define two kinds of beacon messages in our proposed VANET environment. We name those beacons as Regular beacons (*RB*) and Aggregated Beacons (*AB*). *RB* is sent by every vehicle with the frequency of 100-300ms according to DSRC

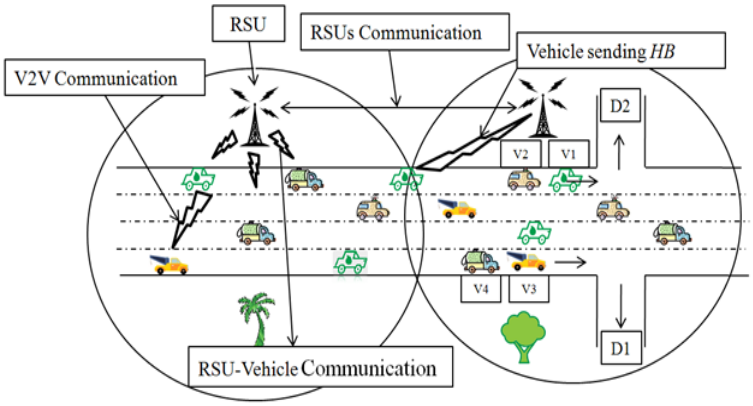

Fig. 2: V-2-RSU and V2V Communication. In V-2-RSU Communication Vehicle is sending beacons to RSU and RSU is sending Aggregated messages to vehicles. RSUs are also sharing information with each other.

standard. In addition to the vehicles, RSUs also receive the beacons and aggregate them into *AB*. By exploiting the properties of VANET, vehicles may have two types of views from the traffic point of view. We define the local view as the view constructed from the regular beacons within the area under one RSU. From the experimental results of Ibrahim et al.'s scheme [4], we assume that the area covered by one RSU may be 1.5 km which means that the regular beacons need to be re-broadcasted. To avoid lingering of beacons forever, TTL may be used and to decide whether a beacon should be re-broadcasted, a timer is used by every vehicle. We assume that timer is used according to probabilistic Inter Vehicle Geocast (*p*-IVG) [5]. Vehicles then extend their view after processing the *AB* from nearby RSU which will contain the traffic density, mean velocity and other information like lane information etc. Our scheme is shown in fig. 2.

3. Conclusion

In this paper, we propose the tradeoff between two conflicting requirements of VANET i.e. privacy and the aggregation. We assumed the presence of densely located RSUs along the road. In addition to other functionalities, RSUs mainly serves two purposes. Firstly, these RSUs receive the normal beacons from the vehicles and by looking at certain bits in the beacon it come to know about the entrance of a new vehicle into its vicinity and the exit. So by this information, RSUs calculate the traffic density. Secondly, the RSUs use the traffic density information to aggregate the normal beacons information into an aggregated message and disseminate it to nearby RSUs and the vehicles as well. Our aggregation scheme is efficient as compared to CASCADE because we do not use any signatures or certificates which bear much cost as compared to symmetric cryptography. Our scheme is also efficient as compared to Park et al.'s scheme in which they use signatures and in addition they disseminate the copies of same message for cross-checking thereby bringing redundancy.

References

[1] M. Raya, and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks", J. Computer Security. 15, 39-68 (2007)

[2] F. Dotzer, "Privacy Issues in Vehicular Ad Hoc Networks", In Danezis, G., Martin, D. (eds) PET 2005. LNCS, vol. 3856, pp. 197-209. Springer, Heidelberg (2006)

[3] R. Hussain, S.J. Kim, H.K. Oh, "Towards Privacy Aware Pseudonymless Strategy for Avoiding Profile Generation in VANET", In Proc. 10th International Workshop on Information Security Applications (WISA2009), (2009)

[4] K. Ibrahim, and M.C. Weigle, "CASCADE: Cluster-based Accurate Syntactic Compression of Aggregated Data in VANETs", In IEEE GLOBECOM Workshops, pp. 1-10. (2008)

[5] K. Ibrahim, M.C. Weigle, and M. Abuelela, "p-IVG: Probabilistic Inter-Vehicle Geocast for Dense Vehicular Networks", In IEEE 69th Vehicular Technology Conference, pp.1-5.(2009)