2012 International Conference on Information and Computer Networks (ICICN 2012)

IPCSIT vol. 27 (2012) © (2012) IACSIT Press, Singapore

PROBLEMS AND THEIR SOLUTIONS WHEN USING GPAS BASED ON VANETs

C. AJIT NATARAJ

IV year, IT SSN College of Engineering , Kalavakam, Chennai

Abstract. Vehicular ad hoc networks, based on vehicle-to-vehicle, vehicle-to-infrastructure communications, promise valuable applications to enhance driving safety, comfort, and efficiency. In this paper we propose the problems and solutions when using GPAS, general purpose automatic survey system based on VANETs. The key motivation of GPAS is to explore the characteristics of data relevance in VANETs: location, time, and user interest. As a new mode to disseminate a survey and collect the required data/responses, GPAS can support a wide range of commercial and traffic-related surveys in a secure, flexible, and cost-effective way. As a preliminary effort, the framework of GPAS is presented in this paper together with in- depth discussions on relevant research challenges and corresponding preliminary solution.

1. Introduction

Vehicular ad hoc networks (VANETs) use moving cars as nodes in a network in order to create a mobile network. Nowadays the massive deployment of VANETs is imminent with the development of VANET technologies (e.g., dedicated short-range communications, DSRC [1], and wireless access vehicular environment, WAVE [2]) underway. Thus, it becomes both necessary and feasible to explore new value added applications for VANETs, such as multi- player games [3] and road surface weather services [4]. Such applications can legitimate the deployment of VANETs and bring about necessary revenues for the further upgrade of VANETs. In this article we thoroughly investigate an automatic survey system based on VANETs, the unique properties of which could better support extensive survey applications.

2. System Architecture

By exploring the relevance of location-based information, GPAS can support various surveys that strictly require responses from a particular region. In addition, GPAS achieves security and privacy by considering different adversary models in VANETs. Here the system overview, network model, survey model and adversary model of GPAS are presented.

GPAS OVERVIEW: There are five main components in GPAS: customers, the survey center, authority, RSUs and vehicular nodes. Survey Center being the central component of GPAS, receives the survey tasks from the customer, registers and obtains necessary authorization from the authority and it assigns the survey requests and proper authorization to the RSUs. GPAS includes the following major procedures.

SURVEY TASK SPECIFICATION: Each customer should specify their survey task to the survey center, including the respondent scope, target region (R_G) as well as the quality requirements to the respondents.

REGISTRATION AND AUTHORIZATION: To ensure security the Survey Center registers one survey at the authority and obtains the authorization for this survey. The authorization's scope is limited to the desired survey activities. To facilitate the dissemination and collection procedures, the

SC may deploy its own RSUs in R_G. Such RSUs are reusable and programmable devices with DSRC-compliant transceivers. The SC also needs to obtain temporary certificates for its RSUs.

DISSEMINATION AND COLLECTION: With the help of RSUs the survey requests will be disseminated to the nodes within R_G. Among these receivers, some may consent to respond to this survey and generate their survey responses. The survey responses will be collected by RSUs, and forwarded to the SC. Here, to encourage nodes to respond to the survey, a certain amount of incentives may be granted to each survey respondent.

SURVEY RESULTS GENERATION: The SC will first pre process the collected survey responses in order to meet the requirements of the customer. Then incentives will be given to confidential survey respondents. The survey responses that are selected as well as the payment agreement among the relevant parties, will be reported to the customers. Proper fees will be charged by the SC for this survey, based on the number of respondents and survey quality. Thus, GPAS is designed to provide customized survey services in a secure, efficient, and effective way based on VANETs.

3. Network Model

VANETs mainly consist of two domains: ad hoc and infrastructure. The *ad hoc* domain is formed by vehicular nodes with DSRC devices, which periodically broadcast beacons to support road safety applications. Each beacon contains the current location, speed, and direction of the sender. Each node is equipped with various pseudonyms to protect its privacy by periodic pseudonym change [7], and a tamper-proof device (TPD) [8] is adopted in each node to keep these pseudonyms confidential. The TPD also ensures that one node can only use one pseudonym at any time.

In the infrastructure domain, all the management functions are abstracted as the *authority* for brevity. The authority is responsible for ID management and trust management for both vehicular nodes and RSUs. RSUs are installed to interface vehicular nodes and the authority. Due to the heavy cost involved, RSUs are only sparsely installed, usually in downtown areas, highway junctions, and so on.

4. Survey Model

In the context of this article, a *survey respondent* refers to either a driver/passenger or a vehicle. A *survey request* refers to the questionnaire for a human or the specification of statistics for a vehicle. A *survey response* is the answers or statistics data from a survey respondent. Based on different survey respondents, we classify various surveys into two types: human oriented (HO) surveys and vehicle oriented (VO) surveys.

HO surveys - HO surveys require the opinions of drivers/passengers on a certain issue that usually is relevant to a region. Thus, human interaction is required for these surveys. An example for this kind of survey is given above .In HO surveys, the respondents (drivers/passengers) will be reached by VANETs, and they will prepare the survey responses at their leisure .Then the responses will be collected when the vehicles are in the range of a dedicated RSU.

VO surveys VO surveys require statistics on the vehicles of a certain model or all vehicles traveling in a region, such as oil consumption. The data can be automatically gathered from onboard sensors installed in each vehicle, so no human interaction is needed. Usually the surveys here are targeted at one specific region, R_G. Thus, in GPAS it is necessary to require that the survey respondents have been to R_G at least once during the survey period, which is referred to as the *spatial condition* of the surveys.

5. Adversary Model

In the process of survey dissemination and collection, some compromised nodes may try to take advantage of GPAS to utilize their personal benefits or to destroy the survey system. Therefore, to ensure

system security we need to identify the adversary model in GPAS. Specifically, even if one node has not gone to the target region, it may still overhear the survey request and generate one response, breaching the spatial condition. Meanwhile, with multiple pseudonyms, one node may generate multiple survey responses and sign them with different certificates.

6. Sc Authorization

SC needs to obtain the corresponding authorization to access and manage VANETs and disseminate survey requests to vehicular nodes upon receiving one survey task from a customer. To this end, for each new survey the SC will authenticate with the authority, and get necessary certificates for itself and its RSUs. The certificate for the SC, explicitly states the scope and duration of the corresponding survey, as well as the authorization for the SC. Short-term certificates will be issued by the authority for the adRSUs to be deployed by SC for this survey. Thus, each adRSU can only send out survey requests and collect survey responses in VANETs, as explicitly stated in the short-term certificate.

7. Survey Request Dissemination

After obtaining proper authorization from the authority, the SC will request the RSUs and adRSUs to disseminate the survey requests to the nodes in R_G. To ensure that the receivers of the survey satisfy the spatial condition, one way is to allow the survey requests to be broadcast only one hop from the RSUs. Obviously, the nodes receiving the survey request must satisfy the spatial condition. In the process of broadcast, some nodes may miss the survey request due to data transmission collisions. To solve this problem, the SC needs to set a suitable broadcast frequency for each adRSU, according to the transmission range and traffic velocity in R_G. Hence, it can make sure all the nodes in the range have the chance to receive the survey request K times (K is up to implementation). The other way to disseminate the survey requests is to implement multi hop broadcast, which can reduce the number of (ad)RSUs needed for the survey request distribution. As in the one-hop broadcast, the SC in multi hop broadcast also determines the broadcast frequency by considering the network dissemination capacity and vehicular traffic. To propagate the requests in multi hop, the nodes receiving the survey requests can implement the contention- based forwarding strategy [9]. In addition, each receiver needs to prove that it satisfies the spatial condition. This can be achieved with a proof solicitation procedure performed by multiple neighbors of the receiver to vouch for one another's current location. Therefore, by these ways, each valid respondent to the HO surveys will be able to prove that it satisfies the spatial condition.

8. Survey Response Collection

For HO surveys, the respondents may answer the survey after several hours or even a few days, so the process of survey response collection may take a longer time. Considering payment for responses, we implement the one-hop collection strategy in GPAS. Once the node is in the range of a RSU, it will send the packet to the RSU with the information: {*Survey_ID*, *Survey_Answers*, *Time*, *Pseud(V)*, *Cert_Pseud(V)*, *Sign_Pseud(V)*}. Here, *Pseud(V)* is the pseudonym of the vehicle *V* send- ing this packet for privacy protection, *Cert_Pseud(V)* is its certificate issued by the authority, and *Sign_Pseud(V)* is its digital signature for this packet. After the RSU has received the survey response, it will send the receipt packet to this node with the information: {*(E_cash)pub lic_key*, *Cert_RSU, Sign_RSU*}. Here, *E_cash* is encrypted with the public key of the targeted receiver, so it cannot be stolen from this node.

Every RSU receiving the survey responses will report all these responses to the SC with the proof of each response and get the corresponding *E cash* which has been paid for the collected responses. Thus, each survey response is accompanied by a proof from the RSU, and both the response and its proof need to be carefully verified by the SC.

9. Survey Response Preprocessing

After collecting a set of survey responses and their corresponding proofs, the SC needs to pre- process them to detect and remove the invalid responses, including :

- The one with incorrect signatures
- The with forged proofs
- Multiple responses generated by the same node

These invalid responses are the potential results of the attacks of some adversaries discussed above. The SC can detect the first two types of invalid responses by simply performing digital signature verification with the authorization obtained from the authority. In order to detect the third type the best method is to submit all survey responses to the authority, and ask the authority whether multiple pseudonyms used in these survey responses are from the same node or not. The SC will clear the duplicated responses. This method, however, is too expensive and does not scale well. Thus, to efficiently manage the responses and satisfy the *quality requirement* discussed above, we adopt random-test-based quality of service (QoS) assurance, shown below, to ensure efficient, secure, and privacy-preserving preprocessing.

Let us assume there are N responses and M misbehaving nodes, each of which sends out two duplicate responses. The SC will randomly select k ($k \ll N$) responses for querying the authority. All N responses are regarded as distinct if there are no duplicate responses in these k responses. Otherwise, the SC will submit all N responses for a full-fledged query. In order to meet the *quality requirement*, k will be selected in such a way that if these k survey responses are all from distinct survey respondents, the probability that there will be less than i duplicated survey responses in all N responses will be larger than $1 - \varepsilon$. Figure 3 shows the relationship of selected responses (k) and invalid responses (i) in the percentage of all N responses when $\varepsilon = 0.01$. The percentage of the selected responses (k) will become less when more invalid responses (i) can be tolerated or the number of total responses N becomes larger. For example, when 2 percent of the invalid responses are allowed, the percentage of selected responses (k) is 1.1 percent when N is 10^4, while it is only 0.112 percent when N is 10^5. Thus, our random test scheme can reduce the overhead caused to the authority, while still meeting a certain quality as specified by the customer.

The misbehaving nodes, if any, will be reported to the authority, and their reputations will be correspondingly adjusted. This indeed is another deterring factor against misbehaving nodes.

10. Vehicle Oriented Surveys

These surveys may include data collection of fuel consumption, commute time, high-fidelity and so on of the vehicles of a certain model. Such information, critical to various applications, is difficult and expensive to collect manually or based on existing survey systems. With GPAS such information can be automatically gathered with high efficiency, accuracy, and reliability.

FUNCTIONS AND CHALLENGES:

In general, the procedures of VO surveys are similar to that of HO surveys except that the survey response collection can be in real time without interaction with drivers/passengers. To perform a VO survey, the survey tasks need to be properly assigned to the target vehicles. Here one challenge is to enable each node to support various VO survey tasks free of drivers' involvement. Another challenge lies in efficiently transmitting the survey tasks to the target nodes. In VANETs, RSUs will only be sparsely deployed, so it is difficult to support VO survey for a given region R_G. Addition to this, in the process of survey response reporting, one challenge is to ensure the *security* of the response and the *privacy* of each respondent. Specifically, the survey responses should be verifiably valid and only accessible to the SC. Meanwhile, in response reporting, each survey respondent should not risk its privacy.

Next, we further specify these functions and challenges in an exemplary scenario of a mandatory traffic survey, which provides useful insights on the support of general VO surveys.

11. High – Fidelity Mandatory Traffic Survey

Here we consider one high-fidelity mandatory traffic survey, where the mobility trace of each node within R_G will be reported to the SC during a certain period. Roadside inductive loops or sensors are quite expensive to deploy and cannot be adopted for on-demand traffic survey in any target region.

GPAS presents a novel solution which consists of several novel components: confining RSUs, mobile code, geo-bound IDs, and QoS-aware data compression.

CONFINING adRSUs :

The adRSUs will be deployed on each exit of R_G, as shown in Fig. 4, so R_G will be isolated from its environment. Each node entering R_G will properly receive the survey task, and each node exiting R_G will be able to quickly report the survey response. This scheme saves much more resources than the simplistic strategy deploying one RSU on each intersection in R_G. Besides RSUs are only temporarily deployed and can be reused later. Here we model R_G as a square area with m roads and n roads in each dimension, respectively. There will be totally mn intersections and $2(m + n)$ exits in R_G. To show the cost reduced by our scheme, the total numbers of adRSUs required by our scheme (C_I) and the simplistic strategy (C_E) are shown in Fig. 5. For any reasonably large m and n, C_I is only a small portion of C_E. For instance, when $m = 50$ and $n = 100$, C_I is 300, only 6 percent of C_E (5000).

MOBILE CODE:

In order to support runtime configuration of vehicular nodes, mobile code [10] will be adopted in GPAS to express and perform the survey tasks. When one node enters R_G, the RSU will transfer the mobile code to this node with proof of authorization from the authority. The mobile code will enable this node to collect the defined statistics and prepare survey responses according to the QoS requirements. When one node leaves R_G, it will transmit all the statistics to the RSU on the exit, and the mobile code will also be revoked by the RSU.

While in R_G, in order to prepare a consistent mobility trace, each node cannot change its pseudonym as usual. A set of geo-bound IDs will be applied to protect each node's privacy. As shown in Fig. 4, when one node with a pseudonym PID enters R_G, the RSU will assign a temporary geo-bound ID. Afterward, this node will use TID in any communications within R_G. When it leaves R_G, the RSU will also return the previous PID back to this node. If the ID exchange procedures at the RSUs are properly designed (as our future work), the privacy of each node within R_G can be properly protected. This is because:

• Any adversary overhearing the communications in RG is not able to link the geo-bound IDs to the normal pseudonyms.

• The customers will analyze mobility traces of the geo-bound IDs instead of the usual pseudonyms.

In this sense, the high-fidelity mobility trace of each node in *RG* will have no negative impact on the privacy of this node.

12. Conclusion

GPAS, being able to support both HO surveys and VO surveys in a secure, flexible, and cost-effective way, promises to be a valuable addition to VANET applications in the imminent deploy- meant of VANETs. The unique challenges to GPAS, as discussed in this article, have all been preliminarily investigated with preliminary solutions proposed accordingly.

13. References

[1] CAMP Vehicle Safety Commun. Consortium, "Vehicle Safety Communications Project: Task 3 Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC," Nat'l. Highway Traffic Safety Administration, U.S. Dept. of Transportation, Washington, DC, 2005.

[2] IEEE 1609.2, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages," July2006.

[3] O. K. Tonguz and M. Boban, "Multiplayer Games Over Vehicular Ad Hoc Networks: A New Application," *Elsevi- er J. Ad Hoc Networks*, vol. 8, issue 5, July 2010, pp.531–43.

[4] B. McKeever and P. Pisano, "Clarus: A Clear Picture," *Thinking Highways (North American Edition)*, vol. 4, issue 4, Nov./Dec. 2009.

[5] M. Schonlau, R. D. Fricker, and M. N. Elliott, "Back- ground on the Survey Process," Ch. 2, *Conducting Research Surveys via E-mail and the Web*, RAND, 2002, pp. 5–18.

[6] A. Angel *et al.*, "Methods of Traffic Data Collection Using Aerial Video," *Proc. IEEE Intell. Transportation Sys. Conf.*, Sept. 2002, pp. 31–36.

[7] Z. Li, Z. Wang, and C. Chigan, "Security of Vehicular Ad Hoc Networks in Intelligent Transportation Systems," *Wireless Technologies for Intelligent Transportation Systems*, Nova Science Publishers, 2009.

[8] F. Kargl *et al.*, "Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges," *IEEE Commun. Mag.*, vol. 46,no. 11, Nov.2008, pp. 110–18.

[9] C. Liu and C. Chigan, "RPB-MD: A Novel Robust Mes- sage Dissemination Method for VANETs," *Proc. IEEE GLOBECOM '08*, Nov. 2008, pp. 1–6.