VEHICLEVIEW: A UNIVERSAL SYSTEM FOR VEHICLE PERFORMANCE MONITORING AND ANALYSIS BASED ON VANETS

ZHENGMING LI, CONGYI LIU, AND CHUNXIAO CHIGAN, MICHIGAN TECHNOLOGICAL UNIVERSITY

ABSTRACT

Ranging from large-scale field testing to remote vehicle diagnostics, vehicle performance monitoring and analysis applications rely on the long-term and large-scale collection of in-vehicle sensor data. With wireless vehicular communications, vehicular ad hoc networks provide a promising platform for such applications. In this article, we propose VehicleView to support the large-scale and long-term collection and mining of in-vehicle sensor data. The system architecture and preliminary procedures of VehicleView are proposed based on comprehensive considerations on the common functional, performance, and security requirements of such applications. Supporting various vehicle performance monitoring and analysis applications in a cost-effective, secure, and privacy-preserving way, VehicleView shows great application potential and economic prospects.

INTRODUCTION

Vehicular ad hoc networks (VANETs) consist of smart vehicles with sensing, computing, and wireless communication capabilities, and roadside units (RSUs), which serve as the smart vehicles' access points to the infrastructure network (e.g., the Internet). Both vehicle-to-vehicle (V2V) and vehicle-to-roadside (V2R) communications are based on dedicated short-range communication (DSRC) technology, which is being standardized as IEEE 802.11p. Similar to WiFi (IEEE 802.11a/b/g/n), DSRC also detects and corrects faulty data in the physical and MAC layers, providing valid data to the upper layers with data rates from 6 to 27 Mb/s.

With V2V and V2R communications, VANETs promise substantial enhancements in traffic safety, traffic efficiency, and driving experience. Specifically, each node will broadcast beacons containing its driving state, such as location, speed, and heading direction, with a period of 100–500 ms [1]. Thus, enabling each node to learn the driving states of the nearby nodes, VANETs support numerous traffic safety applications, such as collision avoidance and lane merge assistance [1]. Besides, real-time traffic statistics can be collected based on V2V and V2R communications, which will improve traffic management and efficiency. Last, V2V and V2R communications can support various value-added applications to further enrich driving experience, such as automatic survey [2], advertising [3], and on-road video game playing [4].

Especially, the potential to improve traffic safety alone is more than enough to justify the cost incurred by the research, development, and deployment of VANETs [5]. Both traffic management applications and value-added applications can be regarded as free-riders. Thus, VANETs may enable more cost-effective solutions to various value-added applications.

Here, we aim to support vehicle performance monitoring and analysis applications based on VANETs. Such applications, including large-scale vehicle field testing, after-sale vehicle performance monitoring, and remote vehicle diagnostics, generally rely on the long-term/large-scale collection and proper mining of in-vehicle sensor data. For instance, by collecting the engine states of vehicles of a particular model over (say) five years, extensive data mining can be performed by car manufacturers to gain important insights into the long-term performance of this vehicle model. Nowadays, several commercial vehicular telematics solutions, such as GM OnStar [6] and Ford SYNC [7], can support such applications. However, these solutions are proprietary systems, which constrain their application scope to specific car manufacturers or fleet owners. Besides, such solutions generally rely on cellular communications (third- or fourth-generation, 3G/4G) for data transmission, incurring service fees to the application users. Besides, with free access to all location and speed states, such solutions impose severe privacy risks to vehicle drivers [8]. At the same time, mainly relying on low-rate near-field communications such as RFID and Bluetooth, the existing toll collection systems are not fit for the long-term and large-scale collection of in-vehicle sensor data either.

1536-1284/12/$25.00 © 2012 IEEE

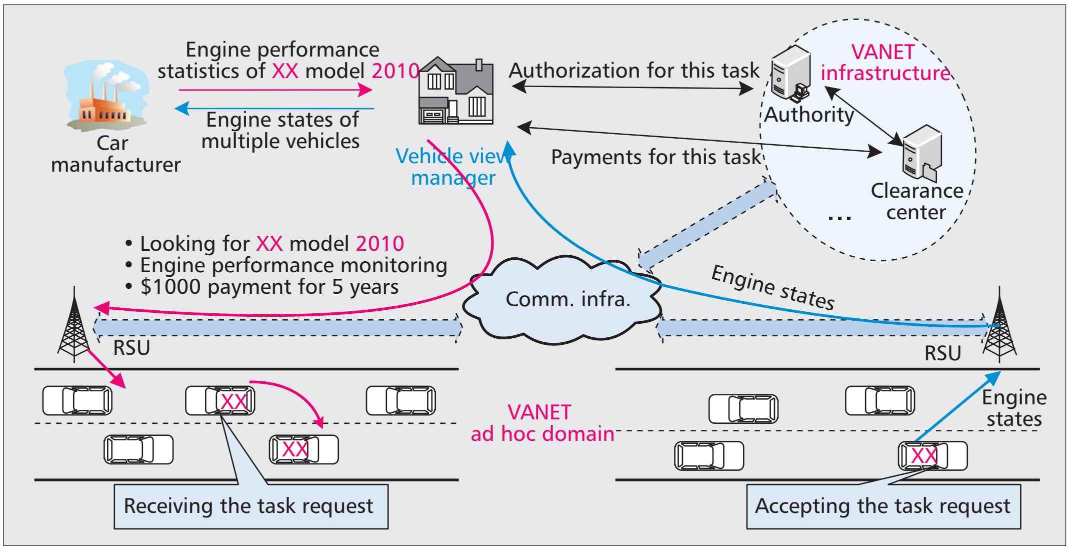
Engine performance statistics of XX model 2010
Engine states of multiple vehicles
Car manufacturer
Vehicle view manager
Authorization for this task
Payments for this task
VANET infrastructure
Authority
Clearance center
...
• Looking for XX model 2010
• Engine performance monitoring
• $1000 payment for 5 years
Comm. infra.
Engine states
RSU
RSU
XX
XX
XX
VANET ad hoc domain
Engine states
Receiving the task request
Accepting the task request

Figure 1. *Exemplary application scenarios of VehicleView.*

In the infrastructure domain, the existing mature communication technologies, such as 3G, 4G, WiMAX, and wired LAN, can be adopted. Thus, generally communications in the infrastructure domain are assumed to be secure and reliable.

Comparatively, VANETs can enable better solutions to these applications with ubiquitous and free V2V and V2R communications. Here, VehicleView is proposed as a universal system for vehicle performance monitoring and analysis applications based on VANETs. Taking advantage of V2V and V2R communications, VehicleView can cost-effectively support in-vehicle sensor data collection and data mining without requiring additional hardware. Moreover, the relevant security and privacy issues are thoroughly investigated in VehicleView, with preliminary solutions proposed. Thus, VehicleView shows salient application potentials and economic prospects by supporting such applications in a cost-effective, secure and privacy-preserving way.

In this article, we first identify and investigate the critical challenges common to vehicle performance monitoring and analysis applications. The overview of VehicleView is then presented with high-level procedures. The critical challenges are further discussed along the proposed solutions, followed by the summaries and our future work.

Background and System Overview

Network Model and Assumptions

In VANETs, the *ad hoc domain* consists of vehicular nodes that periodically broadcast beacons [1] to support road safety applications. Each node is equipped with various pseudonyms to protect its privacy by periodical pseudonym change [9] . In each node a tamper-proof device (TPD) [10] is adopted to keep the pseudonyms confidential, and to allow the use of only one pseudonym at any time. In the *infrastructure domain*, the management functions, including ID management, trust management, and security provisioning, are abstracted as the *Authority* for brevity. Besides, a clearance center (CC) is in charge of the financial transactions in VANETs. Due to cost constraints, RSUs are only sparsely deployed in VANETs. In the infrastructure domain, the existing mature communication technologies, such as 3G, 4G, WiMAX, and wired LAN, can be adopted. Thus, generally communications in the infrastructure domain are assumed to be secure and reliable.

Vehicle Performance Monitoring and Analysis Applications

Exemplary application scenarios of VehicleView is shown in Fig. 1. In general, the major functions of one-vehicle performance monitoring and analysis application include *information requirement determination*, *data items selection*, *target vehicle selection*, *data collection*, and *data mining*. First, the customer (say a car manufacturer) needs to determine the information requirements, for instance, the engine performance degradation curve of a new vehicle model. Based on these, the data items to be collected can be selected from the available in-vehicle sensors, and a subset of vehicles as the data sources will also be selected. Then the required data will be collected from the target vehicles with the help of VehicleView and VANETs. The customer needs to pay a certain incentive to the vehicles to encourage their participation and pay VANETs for their support. Eventually, the customer will mine the collected data to meet its information requirements. All these functions need to be performed efficiently without incurring heavy overhead to VANETs. Moreover, to properly carry out these functions, the security and privacy requirements listed in Table 1 need to be carefully addressed in VehicleView.

VehicleView Overview

As shown in Fig. 2, in VehicleView, the Authority, CC, RSUs, and vehicular nodes are preexisting entities in VANETs. The customer may be a car manufacturer, a research institute, or a government agency, which contains the end user, the performance analysis (PA) controller, and the data center. The data center stores the collected data in a database and performs data mining to answer the queries from the PA con-

	Security	Privacy
Customer	Data reports being intercepted Data reports being tampered Application wrongly initiated by other parties	Data reports being revealed to others
VANET infrastructures	Payment denied by the customer Payment wrongly claimed by nodes	N/A
Vehicles	Payment denied by the customer Data report generation without authorization	ID privacy harmed Location privacy harmed

Table 1. *Security and privacy risks.*

troller. The PA controller converts the PA requirements from the end user to a performance monitoring (PM) task containing tangible data items and quality specifications, and interacts with the VehicleView Manager (VM). The VM is the interface between the customer and VANETs.

The major functional components of VehicleView are designed as shown below.

Task initiation: The end user specifies its information requirements to the PA controller, which will first query the data center and forward the report to the end user if the data center has answers. Otherwise, the PA controller will determine the PM task and send it to VM for further negotiation.

Task negotiation: Upon receiving one task, the VM will evaluate it with policy and economic considerations. An automatic negotiation process will be adopted to allow the customer, Authority and VM to finalize the task and the offered incentives.

Task registration: The VM registers the finalized task in the Authority to get a proper authorization, with which the VM can request related RSUs and the CC to participate in this task.

Task dissemination: The selected RSUs will effectively and efficiently disseminate the task to the target vehicles, based on both V2R and V2V communications.

Data collection: Once deciding to participate in this task, a target vehicle will sample data from its in-vehicle sensors and format the data samples accordingly. The data items will be sent to the nearby RSU, which will forward them to the customer via the VM.

Data mining: The customer performs data mining on the collected data for desired knowledge about vehicle performance monitoring and analysis.

Cash-in: The participants will cash in their earned incentives in the CC, exchanging the incentives for the credits usable throughout VANETs.

Thus, based on V2V and V2R communications, VehicleView only incurs limited software updates to the existing entities. The design challenges and preliminary solutions of these functional components will be elaborated in detail next.

Task Initiation and Negotiation

Task Initiation

To initiate a PM task, the PA controller and the data center will specify the task to meet the information requirements of the end user, based on the available budget and the current data records in the database.

The information requirements of the end user specify the required knowledge and the information quality. The PA controller will first query the data center for possible answers. If the current data records in the data center are not sufficient, the data center will identify the lacking data items in the form of alternative subsets of required data items, each of which can complement the current data records to meet the information requirements. Then it is up to the PA controller to select the suitable data item subset based on the available budget and the future information requirements. Specifically, the PA Controller could either select the data item subset with the minimal cost, or select the one which contains more useful information to cater to the future information requirements without exceeding the available budget, or adopt a mixed strategy.

With the optimal data item subset selected, the task can be specified as:

- The data item subset to be collected (vehicle speed, engine load, etc.)
- Data collection duration
- Data sampling rate
- Number of participating vehicles ($N_{\min}$)
- Whether early quitting of the participants is allowable or not

Task Negotiation

Once the VM receives a task ($Task_i$) from the PA controller, it works with the Authority to check $Task_i$ against security and privacy policies of VANETs and charge a proper price for it.

Here, an *uncertainty principle*, as discussed in detail later, is adopted to protect the privacy of each vehicle. The data item subset of $Task_i$ will be audited regarding the uncertainty principle. If certain data items (e.g., the GPS location trace) violate the uncertainty principle, they will be rejected. Afterward, the data items will be tested by the security policies of access control on the in-vehicle sensors as discussed later. If certain data items are not accessible to the customer, $Task_i$ will also be rejected. Once receiving the rejection of $Task_i$, the PA controller will send the best backup task to the VM for another round of negotiation. As discussed later, most in-vehicle sensors are publically accessible with the consent of the vehicle owners, so in general a reasonable customer will eventually identify a task satisfying the access control requirements.

If $Task_i$ is acceptable, the VM will determine its price together with the Authority, based on the current service load of VANETs, and the data volume and duration of $Task_i$, as discussed later. Eventually, the VM will give a price vector $<Pay_{VM}, Pay_{CC}, Pay_{Au}>$ to the customer, to specify the payments to the VM, CC, and Authority. If the PA controller rejects this price, it will recommend that the end user either increase the available budget or lower the quality requirements.

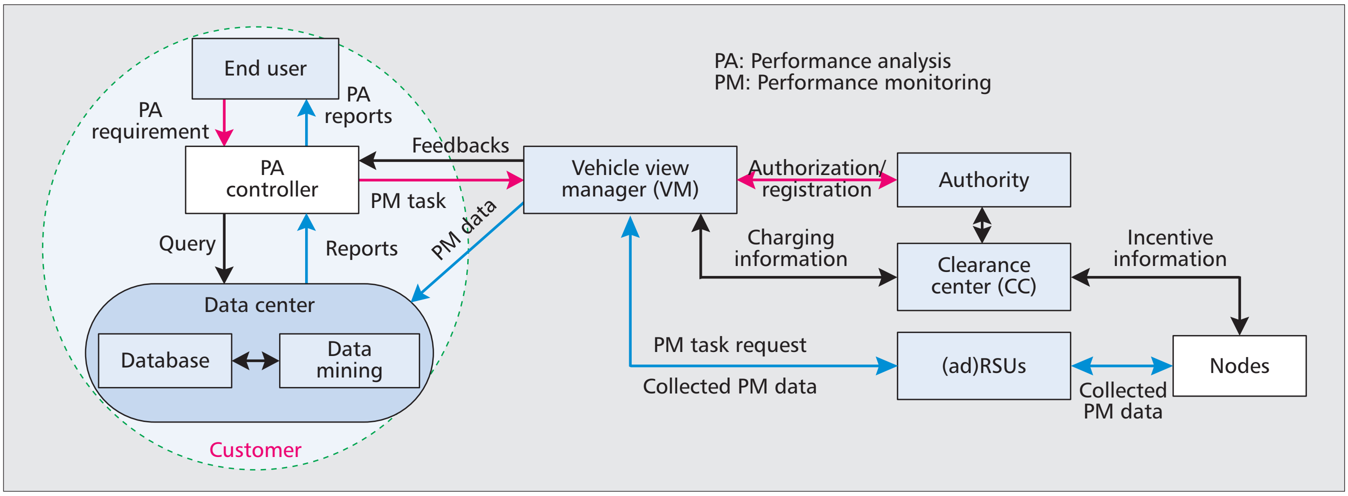

Figure 2. *System overview of VehicleView.*

Thus, task negotiation will allow the customer, VM, and Authority to reach a consensus complying with their respective interests, which makes the task ready for registration.

Data Acquisition and Mining

To collect the required data, $Task_i$ needs to be registered at the Authority, the CC, and involved RSUs. Afterward, $Task_i$ needs to be efficiently and promptly disseminated to the target vehicles to request their participation, and each participating vehicle will report its data from in-vehicle sensors to the customer according to the task specifications. At the data center, data mining will be performed to obtain the desired knowledge.

For clarity, the common notations used below are listed here. $\{message\}PR$ indicates the digital signature of a message generated by a private key PR. $Key\{message\}$ indicates the encrypted message with the public key or secret key (Key). PR_X, PU_X, and $Cert_X$ indicate the private key, public key, and certificate of an entity X, respectively. $H(message)$ is the hash value of *message* generated with a standard hash function such as SHA-2.

Task Registration

VM registers $Task_i$ at the Authority to get a proper authorization, which is given to VM in the form of a certificate as shown below:

$Cert\_Task_i = \{Payload = \{ID_{Task}, H(Secure\_Task), Privileges, Duration\}, \{H(Payload)\}PR_{AU}, Cert_{AU}\}$.

$Secure\_Task = \{Payload = \{ID_{CU}, Content, Eligible\_List, TSP_{CU}\}, \{H(Payload)\}PR_{CU}, Cert_{CU}\}$.

Here, ID_{Task} is the ID assigned to $Task_i$ by the VM. *Privileges* specify the authorized actions of VM regarding $Task_i$: communicating with (a subset of) RSUs and CC. *Duration* indicates the starting and ending time for this certificate. *Secure_Task* is the task content formatted by the customer, where *Content* specifies the data requirements, quality requirements, and pricing information of $Task_i$. *Eligible_List* is an encoded list of the target vehicles. ID_{CU} is the ID of the customer. TSP_{CU} is the timestamp of the customer for *Secure_Task*.

Therefore, with $Cert\_Task_i$, VM is able to register $Task_i$ in RSUs to request their service in task dissemination and data collection. Meanwhile, VM will also register $Task_i$ at CC for the future financial transactions among customer, VM, and Authority regarding $Task_i$.

Task Dissemination

As discussed earlier, the customer may require at least $N_{\min}$ vehicular nodes to persist till the end of $Task_i$. When accepting the task request, the vehicle and VM form a contract for $Task_i$. In case of a binding contract, the initial participants ($N_I = N_{\min}$) will suffice during task dissemination, since each participant is supposed to last through $Task_i$. Otherwise, N_I must be larger than $N_{\min}$ to account for the vehicles quitting halfway. The determination of N_I will be researched in our future work.

With N_I determined, the customer will give a list of target vehicles to VM, which can be a list of vehicle identification numbers (VINs) or a brief description of target vehicles.

In addition, it is challenging to efficiently disseminate the task to the target vehicles, since in VANETs it is difficult to locate a particular vehicle with frequent pseudonym changes. One straightforward method, network-wide flooding, is to flood all the VANETs with the task. Another method, regional flooding, is to allow the VM to obtain the registration locations of the target vehicles so that the VM can select to flood only proper regions to locate the target vehicles. With both methods, V2V communications will be necessary to forward the task over multiple hops.

Here, to preliminarily estimate the communication overhead in task dissemination, we geographically approximate the United States as a 4828 km × 2414 km rectangle that is covered by a huge VANET. Assuming node density is uniform throughout the VANET, for task dissemination, the area to be covered sufficiently indicates the incurred communication overhead. Obviously, a network-wide flooding will cover the entire area of the network. With regional flooding, the area to be covered depends on the number of target vehicles and their daily travel range

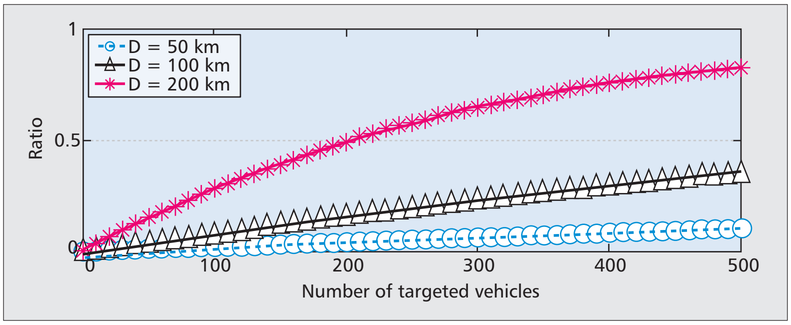

Figure 3. *Saving ratios.*

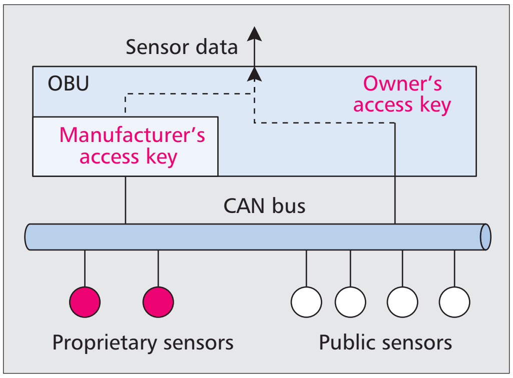

Figure 4. *Layered data access control.*

D. Thus, for each target vehicle, the area to be covered will be πD^2. That is, to disseminate the task to one target vehicle, the circular area with a radius *D*, which is centered on the registration location of this vehicle, will be flooded with the task.

Figure 3 shows the *ratio* of the communication overhead of regional flooding to that of network-wide flooding, which is also the ratio of area covered by the regional flooding to the entire area of the network. As the number of target vehicles increases, the overhead ratio increases quickly. Thus, although efficient with a few target vehicles, regional flooding may not reduce communication overhead much when the number of target vehicles is on the order of thousands. In our future work, task dissemination will be further streamlined to make VehicleView scalable in face of numerous customers.

Secure message exchanges are proposed independent of the task dissemination approach. An RSU will broadcast the task to the nearby vehicles with the following format:

RSU → Vehicles: $Task\_Message = \{Payload = \{Secure\_Task, ID_{RSU}, TSP_{RSU}, Region\}, \{H(Payload)\}PR_{RSU}, Cert_{RSU}\}$.

Here, *Secure_Task* is the same as discussed earlier. ID_{RSU} is the ID of this RSU. TSP_{RSU} is the timestamp of this task message, and Region specifies the region to be flooded with this task.

Upon receiving this task, each node (*A*) will check whether it is eligible for $Task_i$. If it is not the target vehicle, *A* will forward this task to its neighbors through V2V communications, based on the flooding strategies. Otherwise, *A* will decide whether to accept $Task_i$ based on the incentives offered. If *A* decides to accept $Task_i$, it will send a message to the Authority for certification.

A → Authority: $Cert\_REQ = \{Payload = \{SK_1\{ID_{Task}, TSP_A, PU_{CU}\{SK_2\}\}, PU_{AU}\{SK_1\}\}, \{H(Payload)\}PR_{APID}, Cert_{APID}\}$.

Here, SK_1 is used to keep the *Cert_REQ* only accessible to the Authority, and SK_2 is a secret key shared between node *A* and the customer. *APID* is the current pseudonym used by node *A*.

Upon receiving *Cert_REQ*, the Authority will check *A*'s registration information against the *Eligible_List in Secure_Task* to make sure that *A* is eligible for $Task_i$. The Authority will send the eligible node *A*'s registration information to the Customer as follows:

Authority → Customer: $\{Payload = \{SK_3\{PU_{CU}\{SK_2\}, \{VIN, Model, Year\}\}, PU_{CU}\{SK_3\}\}, \{H(Payload)\}PR_{AU}, Cert_{AU}\}$.

Here, SK_3 is a secret key to keep this message only accessible to the customer. Upon receiving this message, the customer will create an entry for node *A* in its database with the information *VIN* and SK_2. In future data collection, SK_2 will be used in encryption of *A*'s data reports. Besides, the customer may from time to time request the Authority to verify that a data report encrypted with SK_2 is really from *A*, which will deter *A* from revealing SK_2 to other ineligible vehicles.

Data Collection

With the cooperation among vehicles, RSUs, and the VM, the required data will be collected and forwarded to the data center. However, data collection extensively involves vehicles and their private data, imposing the severest security and privacy challenges. The conventional security requirements, including data confidentiality, data integrity, and node authorization, can be met by the security procedures described earlier. Besides, access control to the in-vehicle sensors is also critical to VehicleView. Here, a layered data access control framework is proposed as shown in Fig. 4. In each vehicle, the onboard unit (OBU) will only give access to the public sensors with the owner's authorization (in the form of an owner's access key). Both the owner's authorization and the car manufacturer's authorization are needed for OBU to give access to the proprietary sensors. Here, the proprietary sensors may be installed by a car manufacturer for its special tests. A TPD [10] can be adopted in OBU to enforce these access control policies. As such, this framework can better support the specific interests of both car manufacturers and vehicle owners.

For privacy protection, a principle of minimal information revealing is proposed, which requests each party to reveal only minimal information to its interacting parties so as to support the specific functions. For instance, the data reports of the participating vehicles are unnecessary and should not be revealed to the Authority, although their pseudonyms should be revealed to the Authority for identity verification. Besides, the participating vehicles should follow an *uncertainty principle*, which regards the pseudonym history and location history of each node as mutually conflicting. If one party is able to retrieve more pseudonym history of one vehicle, it should only be able to retrieve less location history of this vehicle, so the total uncertainty of both remain larger than a preset threshold. Therefore, with a proper privacy model adopted, the uncertainty principle will ensure proper privacy protection for the vehicular nodes. To enforce these principles, following techniques will be adopted in data collection.

Sparse Enough RSU Deployment — The RSU deployment should be dense enough to support the critical road safety applications, while still being sparse enough to protect the location privacy of each node. A sufficient condition for being sparse enough is to allow more than two alternative RSU-free routes between any two nearby RSUs, so that even the RSUs together cannot figure out the exact travel route of any node. This condition may easily be satisfied at the initial stage of VANET deployment when RSUs will only be sparsely deployed anyway due to the incurred cost.

Delayed Data Reporting — After generating data reports as required, each participant will delay the submission of its data reports for a certain interval. In addition, in each data report only the necessary road profile will be present and the precise GPS locations will not be present. Thus, the location privacy of vehicular nodes can be properly protected in the sense that even with the help from RSUs, the customer cannot figure out the location history of any participating vehicle. Generally, the data for vehicle performance monitoring and analysis applications will be mined in the data center over a long time interval, say, several days, depending on the applications. Thus, delayed data reporting will not harm the concerned applications. In each vehicle, the data reports can be first *mined locally* to reduce information redundancy and message size.

To show the necessity of local (distributed) data mining in VehicleView, here a preliminary estimation is given. Suppose the average speed of one vehicle is 15 m/s, and the communication range is 300 m. Thus, generally one vehicle can only communicate with any RSU for 20 s. The time (t_0) required for a successful data report submission varies greatly in VANETs, which can be up to seconds when the service load is high. Here, for simplicity we assume that on average t_0 is 0.5 s, so each node can only submit 40 (used as the "threshold" in Fig. 5) data reports to an RSU. Meanwhile, the number of delayed data reports, as shown in Fig. 5, may easily exceed this threshold as the average distance among RSUs increases. In Fig. 5, T is the period of data report generation. Thus, local data mining is necessary to make data report submission scalable in VehicleView.

Confidential Data Report — The data report is designed to be both secure and privacy-preserving, as follows:

$A \to \text{RSU}: \mathit{Secure\_Report} = \{\mathit{Payload} = \{\mathit{ID}_{Task}, \mathit{SK}_2\{\mathit{Reports}, \mathit{VIN}\}, \mathit{PU}_{CU}\{\mathit{SK}_2, \mathit{TSP}_{APID}\}\}, \{\mathit{Payload}\}\mathit{PR}_{APID}, \mathit{Cert}_{APID}\}.$

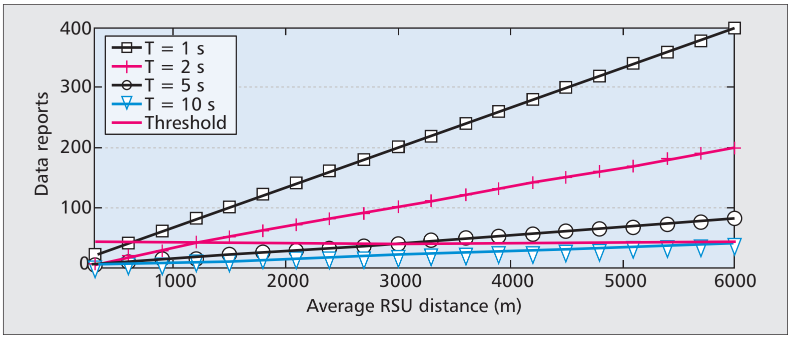

Figure 5. *Accumulated data reports.*

Here, with V2R communication *Secure_Report* will be forwarded to the VM and eventually to the customer. Thus, with SK_2, the data reports are only accessible to the customer. The customer will verify the *VIN* and SK_2 to be sure of the identity of *A*. The customer will also periodically send the *VIN* and $Cert_{APID}$ to the Authority for verifying their proper associations. Besides protecting the data privacy of the customer, this secure data report format can also ensure the data confidentiality, data integrity, and node authenticity requirements.

Data Mining

In VehicleView, two possible forms of data mining exist: *distributed* data mining in each vehicle and *centralized* data mining in the data center. Each participating vehicle adopts distributed data mining to reduce the communication overhead of data collection. Centralized data mining, by contrast, will implement multilevel data generalization, summarization, and characterization to mine the hidden knowledge of the collected data. In the future, concrete algorithms for both distributed and centralized data mining will be designed in the context of specific applications.

Payment Distributions

Here, the pricing model on $Task_i$ is discussed, and the secure distribution of payment is presented.

Pricing Model

Although the concrete pricing model is presented due to the lack of implementation details, the design guidelines are discussed here. As the realistic administrator of VANETs, the Authority holds two objectives regarding VehicleView, service load objective (Obj_1) and revenue objective (Obj_2). The service load objective specifies the desirable service load incurred by value-added applications so that network resource will be properly shared by traffic safety applications, traffic management applications, and value-added applications. The revenue objective specifies the desirable revenues generated by VehicleView so that normal system operations and maintenance can be financially supported.

With these two objectives, conceptually the price vector of $Task_i$ can be determined as $P = (Pay_{VM}, Pay_{CC}, Pay_{Au}) = \text{Pricing}(Task_i, \{\text{Existing tasks}\}, Obj_1, Obj_2)$. Here, $Task_i$ has parameters such as the number of target vehicles (list size), N_I, sampling rate, data report size, and duration. Also, each existing task has its own relevant parameters. The VM and Authority can adjust the impacts of these parameters to achieve the service load and revenue objectives. Once VANETs are deployed, this conceptual pricing model can be easily substantiated with practical considerations.

VehicleView can cost-effectively, flexibly and securely support vehicle performance monitoring and analysis applications, promising great application significance and economic potentials. As the first step, the performance and security (privacy) challenges of VehicleView are identified, with novel solutions preliminarily proposed.

Secure Distribution of Payments

To facilitate exchanges of financial values and protect the privacy of each involved party, E-cash schemes [11] will be adopted for all financial transactions in VehicleView. E-cash enables securely verifiable and anonymous financial operations, where the bearer of an E-cash voucher does not need to present its own identity or prove the source of this E-cash. Besides, E-cash schemes allowing divisible cash operations are especially fit for the customer to distribute payments to various parties.

Assuming that a proper E-cash scheme is adopted, the customer can obtain an E-cash voucher from the CC with a sufficient amount of money. This E-cash voucher can be divided by the customer into vouchers with smaller amount, to pay the VM, CC, Authority, and vehicular nodes. The payment distribution to the VM, CC, and Authority is straightforward, since among them reliable communication connections are available. Because no reliable communication connections exist between the customer and vehicular nodes, payment distribution to these participants will be quite challenging. Since network-wide flooding is too inefficient, here a preliminary solution is provided. Specifically, the customer encrypts the payment to each participant with the shared secret key previously established. Then the encrypted payments are collectively published on a public website, with the task ID (ID_{Task}) as the index. Thus, the participating vehicles can query this website and securely retrieve their due payment.

Summary and Future Work

In this article, VehicleView is proposed as a novel solution to support various vehicle performance monitoring and analysis applications in VANETs. VehicleView allows customers to derive the required data items based on the application requirements through secure and automatic interactions with VANETs. Besides, VehicleView supports secure and efficient task dissemination and data collection from the participating vehicles. Eventually, the economical values can be securely and confidentially represented and distributed to all involved parties, to fully realize the economic potential of VehicleView.

Thus, VehicleView can cost-effectively, flexibly, and securely support vehicle performance monitoring and analysis applications, promising great application significance and economic potential. As the first step, the performance and security (privacy) challenges of VehicleView are identified, with novel solutions preliminarily proposed.

In the future we will design detailed solutions for VehicleView, and perform necessary analytical and simulation evaluation. Thorough discussions on the potential implementation of VehicleView in VANETs will also be given to facilitate the realistic application of VehicleView. With our future work, VehicleView will become an important application system and revenue source for VANETs.

Acknowledgment

This material is based on work supported by the National Science Foundation CAREER award under Grant no. CNS-0644056. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] C. V. S. C. Consortium, “Vehicle Safety Communications Project: Task 3 Final Report: Identify Intelligent Vehicle Safety Applications enabled by DSRC,” Nat’l. Highway Traffic Safety Admin., U.S. Dept. of Transportation DOT HS 809 859, Mar. 2005.

[2] Z. Li, C. Liu, and C. Chigan, “GPAS: A General-Purpose Automatic Survey System based on Vehicular Ad Hoc Networks,” *IEEE Wireless Commun.*, vol. 18, Aug. 2011.

[3] S.-B. Lee *et al.*, “Secure Incentives for Commercial Ad Dissemination in Vehicular Networks,” *8th ACM Int’l. Symp. Mobile Ad Hoc Networking and Computing*, Montreal, Quebec, Canada, 2007, pp. 150–59.

[4] M. Boban and O. K. Tonguz, “Multiplayer Games Over Vehicular Ad Hoc Networks: A New Application,” *Ad Hoc Networks*, vol. 8, July 2010, pp. 531–43.

[5] S. Peirce and R. Mauri, “Vehicle-Infrastructure Integration (VII) Initiative Benefit-Cost Analysis: Pre-Testing Estimates,” Washington, DC, US DoT draft report, 2007.

[6] GM, 2011, OnStar, http://www.onstar.com/web/portal/home.

[7] Ford, 2011, Oct., Ford Sync, http://www.ford.com/technology/sync/.

[8] J. Baugh and J. Guo, “Location Privacy in Mobile Computing Environments,” *Ubiquitous Intelligence and Computing*, vol. 4159/2006, 2006, pp. 936–45.

[9] Z. Li, Z. Wang, and C. Chigan, “Security of Vehicular Ad Hoc Networks in Intelligent Transportation Systems,” Ch. 6, *Wireless Technologies for Intelligent Transportation Systems*, 2009, pp. 133–74.

[10] F. Kargl *et al.*, “Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges,” *IEEE Commun. Mag.*, vol. 46, 2008, pp. 110–18.

[11] D. Chaum, “Blind Signatures for Untraceable Payments,” *Proc. International Crytology Conf.*, 1982, pp. 199–203.

Biographies

ZHENGMING LI (zli1@mtu.edu) received his Ph.D. in electrical engineering from Michigan Technological University in 2012. His research interests include security provisioning, privacy protection, and application design in vehicular ad hoc networks. He got his Master’s degree in engineering in 2005 from Tsinghua University, China.

CONGYI LIU received his M.S. degree in control theory and control engineering from Shanghai Jiao Tong University in China, and he joined the Department of Electrical and Computer Engineering of Michigan Technological University in 2007. Currently, he is working for his Ph.D., and his research interests are focusing on data dissemination, data aggregation, data collection, and their applications in vehicular ad hoc networks.

CHUNXIAO CHIGAN is presently an adjunct associate professor in the Department of Electrical and Computer Engineering at Michigan Technological University and an associate professor in the Department of Electrical and Computer Engineering at the University of Massachusetts Lowell. Her research interests include cyber security and information assurance, vehicular ad hoc networks, cognitive radio networks and security, wireless ad hoc and sensor networks, and vehicle-to-grid (V2G) communications. Her research has been funded by the Department of Defense, industry, and the National Science Foundation (NSF). She received her M.S. and Ph.D. degrees in electrical engineering from the State University of New York, Stony Brook, in 2000 and 2002, respectively. She is a past recipient of the NSF CAREER Award (2007). Currently, she serves as Associate Editor for *IEEE Transactions on Intelligent Transportation Systems*.