Contemporary Engineering Sciences, Vol. 7, 2014, no. 30, 1673 - 1681
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2014.411225

Real-Time Traffic Data Collection Model with Anonymity over Smart Phones

Jeonghee Chi and Soyoung Park[1]

Division of Internet and Multimedia Engineering
Konkuk University, Seoul, Korea

Abstract

We propose a secure and practical architecture to collect traffic data about the entire roadways in real-time by ordinary cars with smart phones. By distributing a mobile vehicular black-box application for smart phones, our model collects image-based traffic information about any roadways by any vehicles using the application. Since each vehicle's traffic data including driving trajectories and patterns are private, we propose an anonymous key-based encryption strategy and an anonymous routing technology in order to prohibit identifying the real vehicle from the communicated data. Additionally, we provide a practical image compression-and-encryption strategy to minimize the communication overheads. Finally, we analyze the efficiency of our image compression method, and simulate the communication performance using NS3 simulator.

Keywords: Real-Time Traffic Data, Vehicular Black-Box Image Communication, Smart Phone, Anonymous Communication

1. Introduction

Intelligent transportation system (ITS) that provides more safe and fluent traffic environments through advanced traffic management are being developed in

[1] Corresponding author

many countries. Among various intelligent transportation technologies, acquisition of correct traffic data about all the roadways in real time is one of the most essential parts for reliable traffic data analysis. Currently, real-time traffic data have been obtained by traffic sensing cameras or other traffic sensors buried in the ground. Since all these devices are statically installed at some particular areas around main roadways, only traffic information around the particular places can be collected and analyzed. In the VANET environment, where the wireless communications among vehicles are allowed, such real-time traffic data collection from moving vehicles would be realistic. However, the main problem is that it will take a long time until the smart vehicles and communication infrastructure adequate for the VANET environment are fully matured.

In this paper, we propose a secure real-time traffic data collection system which can collect traffic data sensed by individual cars on the roads. The main goal is to obtain traffic data about the entire roadways in real-time. To achieve this goal, we develop a mobile vehicular black-box application for smart phones. The mobile application basically provides the black-box functionality for recording vehicle driving routes like other black-box applications. On top of it, our application supports traffic data communication including some extracted black-box images through smart phones. Consequently, our traffic data collection system gathers periodically traffic data of all vehicles using the application. Vehicles can also obtain real-time traffic information about any places of interest in real-time using the application. The best advantage of our model is that it can be simply implemented by currently available ordinary cars with smart phones.

The most two important factors that we have considered to design our system are driver's privacy and data communication efficiency. People will not be likely to provide their black-box images if their driving patterns or driving trajectories may be easily exposed or traced by others unconsciously, even though they could get useful traffic information. Thus, we need a secure mechanism which can collect vehicle's traffic data anonymously. That is, it should be infeasible to identify the real vehicle from the communicated traffic data in our system. Second of all, since our model collects some extracted black-box images along with typical traffic data, we need to develop dedicated communication mechanisms which can minimize both the data capacity and communication overheads. Therefore, we propose a new architecture to collect real-time traffic data from vehicles using a mobile black-box application in this paper, and we also provide both privacy-preserving data communication strategies and efficient image compression-and-encryption mechanisms for its secure use. We describe our system model and the detailed protocols in Section 3 and 4. Finally, we analyze the efficiency of our image compression method, and simulate the communication performance of our model using NS3 simulator. The simulated results will be described in Section 5, and then we conclude the paper in Section 6.

2. Related Work

Related to vehicle black-box image communication, Hong et al. [2] have proposed a black-box evidence collection system, which transmits vehicle's critical video clip to the police station using smart phones for a car accident analysis. Gnanavel [3] has designed another vehicle protection system, which also transmits all sensed signals to the police station. Chi et al. [5] [6] have proposed a practical and secure architecture for vehicular black-box image sharing in VANET. They have introduced several techniques to minimize the communication overheads for transferring and processing black-box images. About the black-box collection system, Park et al. [4] have proposed an intelligent automotive black box mining system to analyze the trajectories of individual vehicles by collecting the location and video information. So far, a secure real-time traffic data collection model based on individual vehicles traffic data has not been proposed yet.

3. System Model

Our system basically consists of our black-box application, smart phones, cars, traffic data collection servers, and a router (or gateway) to play a role of an anonymizer.

Cars are basically supposed to use our black-box application with their smart phones. Thus, cars provide their traffic data along with the corresponding black-box images periodically or occasionally to the traffic data collection server through the application.

The traffic data collection servers consist of two separate servers of TDMS and AMS. TDMS (Traffic Data Management Server) gathers all kinds of traffic data from vehicles, and it keeps updating the traffic DB with up-to-date traffic data for the entire roadways. AMS (Authentication Management Server) performs the tasks of both vehicle authentication and key managements. It manages anonymous keys, and carries out the anonymous key setup protocols with individual vehicles. The anonymous key will be used for traffic data encryption.

We use a specially manipulated router connected to the two servers. The add-on of the router is the function of IP-mixing to hide the real IPs of source vehicles. When a vehicle's data reached the router, it assigns a random IP, and replaces the source IP with it, and sends the modified message to the servers. The sender IP keeps changed at the router for every single transmission.

4. The Proposed Traffic Data Collection System

We illustrate the architecture and operations of our system briefly. Every car that installed our mobile application is automatically registered to the AMS. After the registration, whenever the application is executed, it setups a new anonymous

key with the AMS. The anonymous key is used for traffic data encryption. During the execution of the application, it periodically extracts traffic data, and sends them to TDMS. Of course, whenever some abnormal traffic events happen, the application detects and sends such abnormal events to TDMS server, occasionally. Here, the transmitted traffic data contains some extracted black-box key images, so image compression is performed previously before the transmission. Then, the compressed image is also encrypted with the pre-established anonymous key. During the data transmission, the source vehicle's real IP is randomized by the router before the data are delivered to the servers. Therefore, we forbid it systemically that even the servers identify (or track) the real source from the transmitted data. Now, we give detailed descriptions on each step.

4.1 Registration

The registration is performed automatically when our mobile application is initially installed. The main process of the registration is to setup the membership of each vehicle with the AMS. The application produces its own private-public key pair $<Kv_i^-, Kv_i^+>$, and sends the public key to AMS. Then, AMS generates a pair of member ID and member key denoted as $<MID_i, MK_i>$. Finally, AMS replies with the pair of member ID and key encrypted with the vehicle's public key as follows: $PKE(Kv_i^+, MID_i||MK_i)$, where $PKE()$ means a public key encryption algorithm.

4.2 Key Setup

The application records vehicle's movements like usual vehicle black-box devices during its execution, and in the meantime, it sends periodically some extracted traffic data to TDMS. In order to satisfy both the vehicle anonymity and the data confidentiality in the data communication, it performs a new key setup protocol with the AMS whenever the application is re-started. This prevents that vehicle's driving trajectories or patterns are traced (or tracked) by connecting together all previously spread messages encrypted by the same key. First of all, the AMS maintains a pool of m random keys, and those keys will be refreshed periodically. The random key pool is shared with the TDMS, so the TDMS can always decrypt any ciphers encrypted by one of the keys in the pool. We denote the random key pool at the i^{th} time interval as $KPool_i = \{K_{1,i}, K_{2,i}, ..., K_{m,i}\}$ for $1 \leq i \leq n$. The key ID of $K_{j,i}$ is denoted as $KID_i = j$. Our key setup protocol at the i^{th} time interval is given at Figure 1.

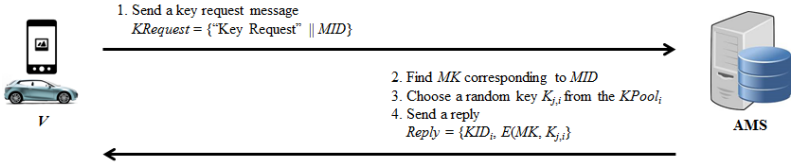


Figure 1. Key Setup Protocol

Vehicle *V* sends a key request message including its master ID. Then the AMS finds the corresponding master key to the given *MID*. Then the server chooses an anonymous key $K_{j,i}$ randomly from the key pool $KPool_i$. And, it encrypts the chosen key with *V*'s master key, and sends it to *V*. *E* () means a symmetric encryption algorithm. Then, *V* will use only $K_{j,i}$ for encrypting its traffic messages in every transmission. The key is named as anonymous key because many different vehicles can be assigned with the same random key. Thus, the server cannot be sure whether the messages encrypted with the same key are generated by the same vehicle, or not. Therefore, our anonymous key provides with the vehicle anonymity as well as data confidentiality.

4.3 Key Frame Extraction

Once the key setup has been accomplished, the application keeps automatically extracting key image frames from the recorded black-box video clip. The extraction occurs in two ways. The basic extraction happens periodically whenever a vehicle passes through a pre-defined interval such like every 100 meter. The second type of extraction occurs occasionally when abnormal traffic events have been detected. The abnormal traffic events, such as car accidents, traffic jam, road construction, and so on, can be detected either automatically by the application, or manually by driver. Since the automatic abnormal event detection is out of scopes of this paper, we will remain it for our future work.

4.4 Image Compression and Encryption Hybrid

The capacity of the extracted key image is up to several megabytes from a few hundreds bytes depending on the image resolution. Thus, we need an image compression mechanism, which can maximize the compression rate while minimizing the data loss. Since most black-box images have a regular style as shown in Figure 3, we propose an ROI (Region of Interest)-based image compression strategy. We divide a selected frame into three sub-regions as center, around, and background, and then compress each region with different compress rates. As shown in Figure 2, the center is the midst region of the image that shows a specific traffic situation most clearly, and so that it should be compressed with the least loss of data. The around is the area around the center that mainly contains roads and other neighboring cars. This area is relatively less important than the center, so the more loss of data can be tolerable. The background is the rest of image including all the other landscapes near the streets, so the loss of data can be the most tolerable.

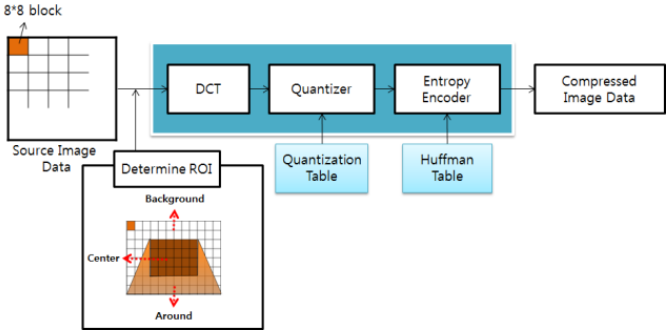


Figure 2. ROI based JPEG Encoder Processing Step

For fast and efficient image compression, we use a modified JPEG compression technique as shown in Figure 2. The input image is divided into 8 by 8 blocks, and three sub-regions are determined. Then, the discrete cosine transform (DCT) is applied to each 8x8 block. The two dimensional DCT is computed for each block by the following equation (1). (u, v) is the index of each pixel in a single block.

$$D(u,v) = \frac{1}{4}C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7} p(x,y)cos\left[\frac{(2x+1)u\pi}{16}\right]cos\left[\frac{(2y+1)v\pi}{16}\right], C(\gamma) = \begin{cases} \frac{1}{\sqrt{2}} & if\ \gamma = 0 \\ 1 & if\ \gamma > 0 \end{cases} \quad (1)$$

The DCT coefficients D_q (u, v) are then quantized by the element quantization table Q (u, v) and a pair of weights α and β according to the sub-regions as following:

$$D_q(u,v) = \begin{cases} round\left\{\frac{D(u,v)}{Q(u,v)}\right\} & if\ D(u,v)\ is\ within\ Center \\ round\left\{\frac{D(u,v)}{Q(u,v)+\alpha}\right\} & if\ D(u,v)\ is\ within\ Around \\ round\left\{\frac{D(u,v)}{Q(u,v)+\beta}\right\} & otherwise \end{cases} \quad (2)$$

Finally, the DCT coefficients are ordered by ZIG-ZAG, and then coded by Huffman encoding method [1]. The Figure 3 shows the examples of our image compression.

(1) Original Image (336 kb)

(2) Compressed Image (90 kb)

Figure 3. The Example of the ROI-based Image Compression

Each compressed key frames is encrypted before transmitting. The entire compressed image is encrypted with the pre-established anonymous key $K_{j,i}$. Any symmetric encryption algorithms, such as 3-DES, AES, etc., can be used for the encryption.

4.5 Privacy-Preserving Data Transmission

Finally, the application sends the compressed-and-encrypted key frame, denoted as *CipherImage*, along with the corresponding traffic information to the TDMS as follows:

$$TMessage = KH(KID_i, Timestamp) \| CipherImage \| E(K_{j,i}, Info) \| Timestamp$$

where *Info* is a set of traffic information including GPS points, speed, event type, etc. *KH* () is a keyed hash function. This is to hide the real key ID from the message. Whenever TDMS receives *TMessage*, TDMS finds the anonymous key of the given KID_i in the *KPool* by hashing all key IDs with the given timestamp, and decrypts both *CipherImage* and the traffic information with the key. The original black-box image and its corresponding traffic data are stored at the server.

Here, even though each vehicle's data are encrypted by the indistinguishable anonymous key, the IP of sender is almost static during the execution of the application. So, TDMS may be able to link together messages given from the same source IP. Therefore, we propose to use a dedicated router connected to the servers for randomizing the IPs of vehicles. That is, whenever each vehicle sends its message to either AMS or TDMS, the real IP of the source vehicle is replaced with a random IP at the router before the message arrives at the destination server. Thus, the source IP is changed in every single transmission. Figure 4 illustrates the concept of our routing mechanism.

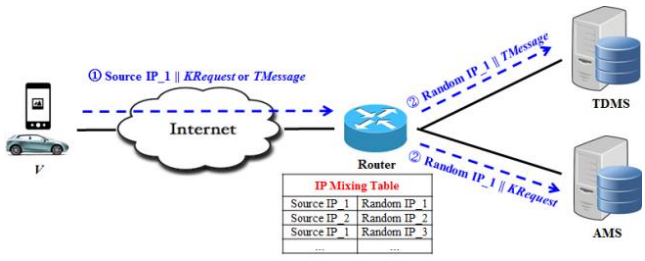


Figure 4. The Operation of Our Manipulated Router

In order to provide stronger security, the random IP can be stored by encrypted with router's selected key. Even though the IP mixing table would be exposed outside, it is infeasible to find the real source IPs associated with the known random IPs. In addition, in order to prevent the man-in-the middle attack between vehicles and the servers, [7] can be applied to our system.

5. Simulated Performance

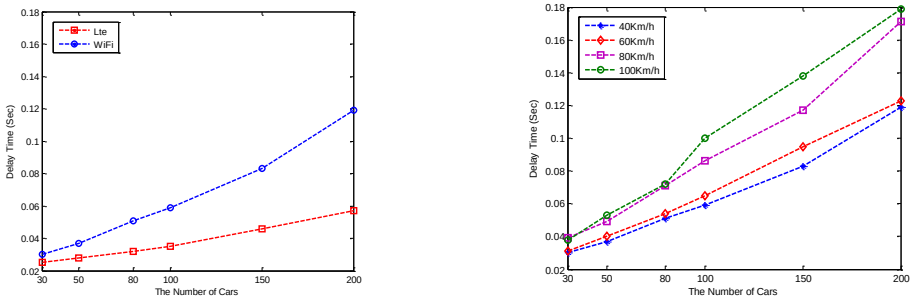
First of all, we analyze the efficiency of our image compression method. We have used 6 video clips with different resolutions, and 20 key frames for each black-box clip have been used in the test. Table 1 summaries the compression rate and processing time.

Table 1. Summary of Image Compression

Data Set	Resolution	AVG Size of Original Image (Kb)	Standard Deviation of Original Image (Kb)	AVG Size of Compressed Image (Kb)	Processing Time (ms)
Clip 1	200*112	50.25	14.97	2.7	84.25
Clip 2	400*225	93.88	20.42	6.85	321.4
Clip 3	640*360	165.92	34.86	14.45	838.75
Clip 4	800*450	229.45	50.74	21.95	1298.6
Clip 5	1024*576	309.60	65.30	34.05	2080.95
Clip 6	1920*1080	576.35	379.82	102.35	7069.15

The compression ratio is over 90% in most cases, and the processing time is less than 1 second for images with the resolution of 800*450 and under. We can conclude that the proper resolution of key images is around 800*450.

Second of all, we analyze the communication delay of our proposed model. Since only smart phone communications are allowed, either the data network (LTE) for smart phones or WiFi network can be used. In the simulation, 30, 50, 80, 100, 150 and 200 cars are used, and cars are supposed to move with different speeds of 40km/h, 60km/h, 80km/h and 100km/h. Figure 5 shows the communication delays in both networking environments. The communication delay in LTE is more than 30% less than the WiFi. And the delay in the WiFi is more affected by the speeds whereas the delay in LTE is not affected by the speeds. The delay in LTE with a density of 100 vehicles moving by 40km/h is 0.035 seconds, and the delay in WiFi with the same situation is 0.059 seconds. As the speed increases up to 100km/h, the delay in WiFi increases to 0.1 seconds.



(a) Communication delay for the speed of 40km/h (b) Communication delay in WiFi according to Speeds

Figure 5. Communication Delay

6. Conclusion

In this paper, we have proposed a secure real-time traffic data collection system which can collect traffic data sensed by individual cars on the roads. Using with a mobile vehicle black-box application, the traffic data collection servers obtain not only typical traffic information but also the corresponding black-box images from cars in real-time. In order to collect individual vehicle traffic data securely, we have provided both an anonymous key-based data encryption method and privacy-preserving data communication strategies. In addition, we have proposed efficient image compression- and-encryption mechanisms to minimize the communication overheads. We will continue to studying about the automatic abnormal traffic detection based on driving patterns.

References

[1] C. Yun, S. Ko and G. Lee, The Study about the Differential compression based on the ROI (Region of Interest), Journal of the Korea Institute of Information and Communication Engineering, Vol. 18, No.3, pp.679 - 686, **(2014).** http://dx.doi.org/10.6109/jkiice.2014.18.3.679

[2] C. Hong, T. Le, K. Chae and S. Jung, Evidence collection from car black boxes using smartphones, Proc. of Consumer Communications and Networking Conference, pp.836 - 837, **(2011)**. http://dx.doi.org/10.1109/ccnc.2011.5766619

[3] G. Gnanavel, Embedded based complete vehicle protection, International Journal of Scientific & Technology Research, vol. 2, no. 4, pp.176-178, **(2013)**.

[4] H. Park and D. Ko, A Design of the Intelligent Black Box using Mining Algorithm, International Journal of Smart Home, Vol.6, No.2, **(2012)**.

[5] J. Chi, H. Park and S. Park, The Architecture for Vehicular Black-Box Image Communication in VANET, Proc. of the IEEE International Conference on Ubiquitous and Future Network (ICUFN), **(2014)**.

[6] J. Chi, J. Kim, S. Do and S. Park, A Group-based Vehicular Black-box Image Sharing Model Using Smart Phones in VANET, Contemporary Engineering Sciences, Vol.7, no.13, pp.629 - 635, **(2014)**.http://dx.doi.org/10.12988/ces.2014.4669

[7] R. Kumar, S. Verma and G. S. Tomar, Thwarting Address Resolution Protocol Poisoning using Man in the middle Attack in WLAN, International Journal of Reliable Information and Assurance, Vol. 1, No. 1, **(2013)**

Received: October 1, 2014; Published: December 2, 2014