Contemporary Engineering Sciences, Vol. 7, 2014, no. 13, 629 - 635
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2014.4669

A Group-based Vehicular Black-box Image Sharing Model Using Smart Phones in VANET

Jeonghee Chi, Jieun Kim, Sunyoung Do and Soyoung Park[1]

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

Abstract

In this paper, we introduce a new practical and secure architecture for vehicular black-box image sharing in VANET, which consists of black-box equipped vehicles, roadside units (RSUs) and a centralized traffic image control server (TICS). In our model, all vehicles that registered to TICS provide with their black-box images to TICS so that TICS manages all traffic images about the entire roads. Then, the vehicles can obtain up-to-date traffic images for any locations from TICS in real-time. For its efficient and secure use, we propose an RSU-assisted communication mechanism to minimize the communicational overheads, and anonymous authentication protocols for preserving vehicle's privacy. We also analyze the efficiency of our model using NS3 simulator.

Keywords: Vehicular Black-box Image Communication, VANET, RSU

1. Introduction

Recently, black-box equipped vehicles are rapidly increasing despite its high cost, because the black-box images are used as evidence for making correct decisions on car accidents. Unlike text messages, black-box images show more detailed descriptions for a particular traffic situation, so more accurate traffic analysis is available. In a VANET environment where V2V (Vehicle to Vehicle) or V2I (Vehicle to Infrastructure) communications are allowed, vehicles may obtain every traffic situational images on the

[1] Corresponding Author

entire roadways by communicating with their black-box images. Thus, real-time traffic analysis on every roadway will be available. In this paper, we introduce a new practical architecture for the vehicular black-box image communication, which satisfies efficiency, security and availability. The primary goals are: (1) minimize the communicational overheads for sharing the vehicular black-box images; (2) make vehicles obtain up-to-date traffic images instantly; and (3) make only reliable black-box images exchanged anonymously. To accomplish all these goals, we propose two layered group-based vehicular black-box communication model, which consists of black-box equipped smart vehicles, roadside units (RSUs) and a centralized traffic image control server (TICS). All vehicles, who registered to TICS, provide with their black-box images periodically to TICS during driving. TICS manages up-to-date traffic images for every roadway. The vehicles can also obtain latest traffic images for any locations of interest from TICS. In order to minimize the communicational and computational overheads between vehicles and TICS, we propose an RSU-assisted communication model, which uses RSUs as intermediate access points between vehicles and TICS. Two main tasks of RSUs are relaying data between vehicles and TICS and authenticating the membership of the vehicle on behalf of TICS. Consequently, a vehicle's data are sent to a near RSU at first. The RSU authenticates the vehicle's membership, and then, delivers only verified vehicle's data to TICS. TICS's replies are also sent back to the vehicle through the RSU. Since the authentication of each vehicle is carried out by distributed RSUs, the computational overheads at TICS can be dramatically reduced. In addition, we propose an anonymous authentication mechanism in order to protect vehicle's identification in the membership authentication process.

Our concrete system model and additional detailed protocols and algorithms will be described in Section 3 and 4. We will analyze the communicational efficiency of our model using NS3 simulator in Section 5 and finally conclude the paper in Section 6.

2. Related Work

Most researches related to vehicular black-box [1-5] are focused on developing intelligent recording systems with high performance for detecting and simulating abnormal vehicular situations or events with advanced controllers or diverse vehicular sensors. Related to the black-box image sharing, Hong et al. [6] 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 [7] has designed another vehicle protection system, which also transmits all sensed signals to the police station. Related to video image transmission, researches for seamless black-box video streaming services in VANET [8-10] have been provided. As long as we know, the research for sharing vehicular black-box images with other vehicles to obtain traffic images for any locations has not been proposed yet, and we propose it newly.

3. Assumptions, System Configuration and Notations

Our system consists of smart vehicles, RSUs and TICS in a VANET environment. Smart vehicles are supposed to be equipped with sensors for sensing neighboring traffic situation, OBU (On Board Unit) for data storage and computation, networking devices, and GPS, etc. Any black-box equipped ordinary vehicles can utilize VANET-like services using smart phones in our model because a smart phone supports all above functionalities on behalf of the smart vehicle's OBU. Vehicle's black-box images can be sent to a smart phone periodically by the Bluetooth communication.

RSUs are static units equipped with storage, a computational device and a transmitter for wireless communications. Every RSU is managed by Certificate Authorities (CA) so that it has its own public key pair and its certificate. RSUs also store other RSU's public keys. RSU can generate a digital signature on some messages with its key pair. Vehicles can also obtain the CA's public key at any time.

TICS is a centralized server to manage all traffic images gathered from vehicles. We assume that TICS can communicate with every RSU by either wired or wireless communications. TICS updates traffic images for every roadway continuously, and provides with up-to-date traffic images to the requests of vehicles. The notations used though the entire paper, are summarized in table 1.

Table 1. Notations

Notations	Descriptions	Notations	Descriptions
MID_i, MK_i	A member ID and key pair of v_i	$Sig(K^-, M)$	Digital signature on a message M with a private key K^-
Kv_i^-, Kv_i^+	A private and public key pair of v_i	$E(K, M)$	A symmetric encryption on M with a key K
TK_i^-, TK_i^+	A temporary private and public key pair of v_i	$PKE(K^+, M)$	A Public key encryption on M with a public key K^+
KR_i^-, KR_i^+	A private and public key pair of R_i	$H(M)$	A cryptographic hash function on a message M

4. Vehicular Black-Box Image Sharing Scheme

Now we explain our anonymous authentication mechanisms and communication strategy in detail in the following subsections.

4.1 Member Registration and Anonymous Authentication

Any vehicle can register to TICS by installing the corresponding mobile application at its smart phone. The main process of the registration is to create each vehicle's member ID and member key. Let a vehicle be v_i. v_i creates its own private-public key pair $<Kv_i^-$, $Kv_i^+>$, and registers Kv_i^+ to TICS. TICS creates v_i's member ID and key denoted as $<MID_i$, $MK_i>$, and sends them as encrypted as follows: $PKE(Kv_i^+, MID_i||MK_i)$.

Whenever v_i passes by RSUs, v_i sends its black-box data to send them to TICS. If v_i keeps using its member ID and key for its authentication whenever it sends data to TICS, TICS can easily trace v_i's moving trajectories from the unique ID. In order to figure it out, we use a concept of chained authentication by RSUs. Once v_i is initially authenticated by an RSU with its member ID and key, the RSU gives an authentication token to v_i. Thereafter, whenever v_i reaches a next RSU, v_i shows the authentication token to the RSU. The RSU verifies only the validity of the authentication token, that is, verifies that v_i has been already authenticated by a previous RSU. If verified, the RSU assigns with a new authentication token for next authentication. In this way, vehicles can be authenticated by RSUs without exposing its member ID and key. After finishing the authentication, each RSU signs the vehicle's data except for the vehicle's identification data, and forwards the modified data to TICS. Finally, TICS verifies the RSU's signature and updates the traffic images, so it cannot identify the source vehicle. The detailed protocols for our chained authentication are given below.

(1) Initial authentication: The initial authentication occurs once at the firstly reached RSU, denoted as R_j. The initial authentication needs the cooperation of TICS to verify that v_i is a registered member to TICS. R_j is supposed to broadcast its ID RID_j and a random nonce N_j periodically. The detailed protocol is given in Figure 1.

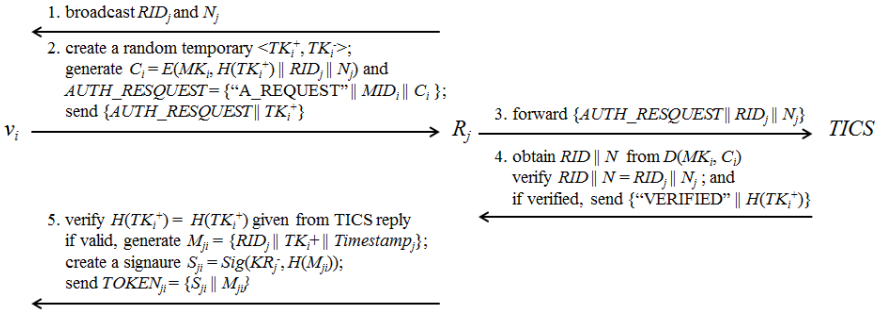


Figure 1. Initial authentication

v_i creates a temporary key pair $< TK_i^+, TK_i^- >$. And v_i encrypts its hashed public key and the RSU information with its MK_i. R_j forwards v_i's message with the same RSU information to TICS. TICS decrypts the message and compares v_i's message with R_j's message. If verified, R_j sends an authentication token, which is R_j's signature on TK_i^+.

(2) Chained authentication: Let v_i's black-box data be D_i. v_i continues the chained authentication with upcoming RSUs, denoted as R_k as follows:

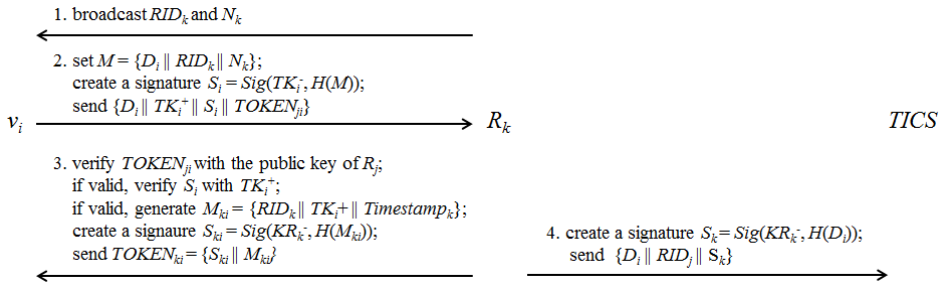


Figure 2. Chained authentication

v_i makes a signature on D_i with TK_i^- and attaches R_j's $TOKEN_{ji}$ show that TK_i^+ is authenticated by R_j. R_k verifies $TOKEN_{ji}$ with R_j's KR_j^+ and verifies S_i with TK_i^+. If both signatures are valid, then R_k creates a new token $TOKEN_{ki}$ for TK_i^+. Here, the valid period of the *TOKEN* is very short, so vehicles should update the *TOKEN* whenever it passes by an RSU. Finally, R_k forwards D_i signed by R_k to TICS. Since every vehicle's data are signed by RSUs, TICS cannot distinguish the real vehicle that generated those images.

4.2 Traffic Image Communication Strategy

In this section, we describe our black-box image communication mechanism, which can minimize the communicational overheads.

4.2.1 Vehicle's Key Frame Extraction

Vehicles provide only selected key frames together with the corresponding GPS points to TICS. The key frames are selected by two policies: event-based extraction and image-based extraction. By the event-based policy, any abnormal behaviors of vehicle, including sudden brake or accidental lane change are regarded as events. Thus, whenever such events happen, the corresponding black-box images are extracted as key frames. The image-based key extraction extracts distinct static images by checking the similarity between consecutive frames. We use our preliminary result of the image similarity check algorithms [10] for the image-based key frame extraction.

4.2.2 Traffic Image Communication on Demand

Lastly, any registered vehicle can ask for up-to-date traffic images about particular locations to TICS. To do this, the vehicle, denoted as v_i, makes a request for the locations based on the GPS points, and broadcasts it. An RSU that received the request for the first time, denoted as R_k, determines the membership of v_i. If valid, R_k sings the request and sends the modified request to TICS in order to conceal v_i. Finally, TICS replies to R_k with the corresponding images after verifying R_k's signature. Here, the replies should be shown to v_i only, so the reply is encrypted. The detailed protocols are given below.

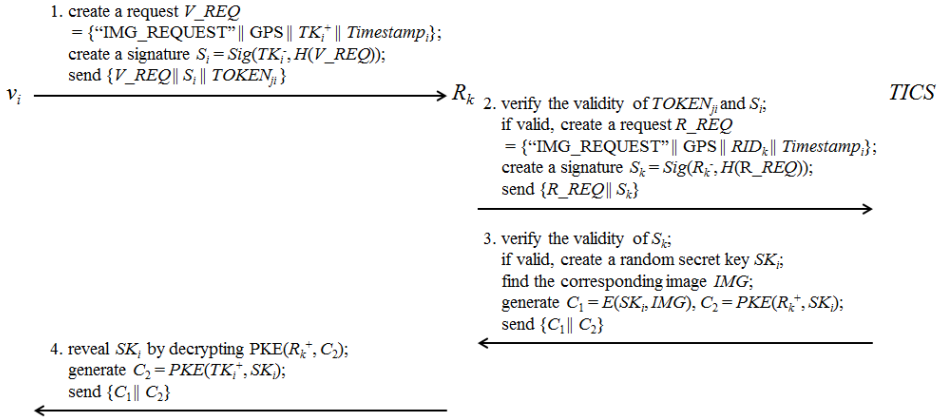


Figure 3. Protocol for traffic image communication on demand

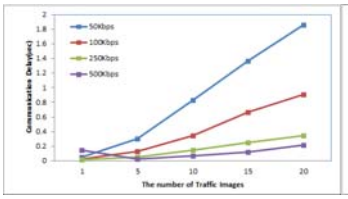
v_i sends a signed request and $TOKEN_{ji}$ to R_k. If both the token and S_i are valid, R_k replaces S_i with its signature S_k, and sends the modified request to TICS. If S_k is valid, TICS replies with the image *IMG* corresponding to the given GPS. *IMG* is encrypted with a randomly chosen symmetric key SK_i as follows: $E(SK_i, IMG) = SK_i \oplus IMG_n$ for $n=\{1,....,m\}$, where IMG_n is the n^{th} block of *IMG* and the block size is identical to the key size. The goal of encryption is just for hiding the exact contents to unregistered vehicles, a simple image encoding technology has been used for the efficiency. SK_i is delivered to R_k encrypted with R_k's public key. R_k reveals SK_i and resends the reply and the SK_i by encrypting with v_i's TK_i^+. Consequently, the only v_i except R_k can reveal *IMG*.

5. Simulated Performance

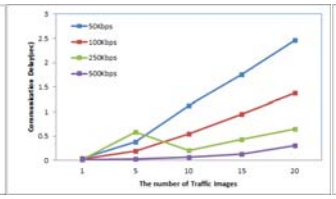
In this section, we provide our simulation results. We have used 5 RSUs with a transmission range of 250m and 20 vehicles randomly moving with an average speed of 60km/h. A vehicle can ask to TICS up to 20 different traffic images. The size of each traffic image is 15Kbyte. We have analyzed the communication delay between the vehicle and TICS for different network bandwidths of 50, 100, 250 and 500 Kbps.

Figure 4(a) shows the delay according to the number of traffic images requested by a vehicle. For a single traffic image, the delay is 40ms for 50 Kbps but 18ms for 250 Kbps. In the case of asking traffic images for 10 different locations, the delay is 820ms for 50 Kbps but 143ms for 250 Kbps. We could find that the delay in the worst case is still tolerable for the successful traffic image communication. Figure 4(b) and (c) show the results for the case that multiple requests are delivered to TICS simultaneously. For the worst case analysis, each vehicle asked 20 traffic images. For 250 Kbps, the delays are 640ms and 1101ms for the cases of 4 requests and 6 requests, respectively. But, for 500kbps, the delay is 346ms in the worst case. Figure 5 shows the delay according to

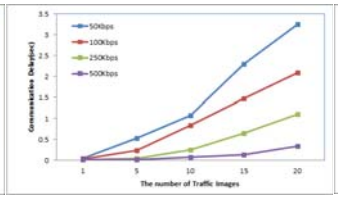
bandwidth. With 500kbps, the delay is less than 350ms for every case. The delay for asking 10 images is around 1 second in any cases. Thus we can conclude that our model can work successfully even in the networking environment having very low bandwidth.



(a)The # of requests = 1



(b) The # of requests = 4



(c) The # of requests = 6

Figure 4 Communication delay according to the number of traffic images

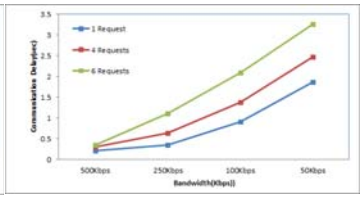


Figure 5 Communication delay according to bandwidth (The # of traffic images = 20)

6. Conclusion

We have proposed a practical and secure architecture for vehicular black-box image sharing in VANET. We have suggested an RSU-assisted communication model between vehicles and TICS and an anonymous authentication protocols that can authenticate each vehicle's membership without identifying the vehicle. We have simulated the communication delay of our model, and the results show that our model can work efficiently for its practical use. We still need to improve our model to reduce the computational costs for the anonymous authentication.

Acknowledgements. This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the Seoul Accord Vitalization Program (NIPA-2014-H1807-14-1017) supervised by the NIPA (National IT Industry Promotion Agency).

References

[1] A. Kassem, R. Jabr, G. Salamouni and Z. Maalouf, Vehicle black box system, Proc. of the Annual IEEE Systems Conference, pp.1-6, **(2008)**.
[2] L. Jiang and C. Yu, Design and implementation of car black box based on embedded system, Proc. of the International Conference on Electrical and Control Engineering, pp.3537-3539, **(2010)**.
[3] O. S. Siordia, I. M. Diego, C. Conde and E. Cabello, Wireless in-vehicle complaint driver environment recorder, Proc. of Signal Processing and Multimedia Applications Conference, pp.52-58, **(2011)**.
[4] O. S. Siordia, I. M. Diego, C. Conde and E. Cabello, Accident reproduction system for the identification of human factors involved on traffic accidents, Proc. of the IEEE Intelligent Vehicles Symposium, pp.987–992, **(2012)**.
[5] G. Nowacki, A. Niedzicka and C. Krysiuk, The use of event data recorder (EDR)–black box, Advances in Science and Technology Research Journal, pp.62-72, **(2014)**.
[6] 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)**.
[7] G. Gnanavel, Embedded based complete vehicle protection, International Journal of Scientific & Technology Research, vol. 2, no. 4, pp.176-178, **(2013)**.

[8] N. Kumar and J. Kim, Probabilistic trust aware data replica placement strategy for online video streaming applications in vehicular delay tolerant networks, Mathematical and Computer Modeling, pp.3-14, **(2013)**.
[9] C. Lee, C. Huang, C. Yang and H. Lin, The K-hop Cooperative Video Streaming Protocol Using H. 264/SVC over the Hybrid Vehicular Networks, IEEE Transactions on Mobile Computing, **(2014)**.
[10] C. Rezende, A. Mammeri, A. Boukerche and A. A. Loureiro, A Receiver-based Video Dissemination Solution for Vehicular Networks with Content Transmissions Decoupled from Relay Node Selection, Ad Hoc Networks, **(2014)**.
[11] 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), to be appeared, **(2014)**.

Received: May 1, 2014