Computer Science and Information Technology 3(3): 59-65, 2015 http://www.hrpub.org
DOI: 10.13189/csit.2015.030301

A Preference-based Privacy Protection for Value-added Services in Vehicular Ad Hoc Networks

Iuon-Chang lin[1,2,*], Yi-Lun Chi[3], Hsiang-Yu Chen[1], Min-Shiang Hwang[3]

[1]Department of Computer Science and Engineering, National Chung Hsing University, Taiwan
[2]Department of Photonics and Communication Engineering, Asia University, Taiwan
[3]Department of Computer Science and Information Engineering, Asia University, Taiwan

Abstract Due to the rapid growth of smart devices, the development of VANET tends to mature. Although many methods have been proposed to resolve the user privacy issue in vehicular ad hoc network (VANET), users still didn't know what information is collected (e.g. geolocation) and how to use .In this paper, we propose a secure and anonymous scheme for communication, which is based on blind signature techniques, and user can set their own privacy preferences before joining the VANET. Our proposed scheme lets user know whether his/her privacy preferences is suitable for VANET environment, and provide appropriate value-added service to user. Finally we will show our proposed scheme meets various security requirements.

Keywords Vehicle Ad Hoc Networks, Privacy Preference, Anonymity, Value-added Services, Blind Signature

1. Introduction

Many countries and enterprise have been devoted to the Internet of Things (IoT) domain targeting smart transportation concept, for various reasons. The main one is the rapid growth of smart devices, which have been embedded sensors to automatically transfer data over communication networks [1]. The second reason is the number of vehicles increasing continually, and it causes many traffic problems, such as traffic congestion, parking problem and accidents.

Recently, Vehicle ad hoc network (VANET) becomes a popular research topic in academia and many countries; it plays a critical role to develop Intelligent Transportation System (ITS) [18]. In a typical VANET, each vehicle has been installed on-board unit, and there are many roadside units have been deployed along the roads. There are two communication modes in VANET: vehicle-to-vehicle communication (V2V) and vehicle-to-infrastructure communication (V2I). In V2V mode, each vehicle can communicate with other nearby vehicles; in V2I mode, vehicles can communicate with neighboring RSUs or base station. VANET have been utilized for vehicles broadcast safety message. For example, if there is the accident happened on the road, the ambulance can broadcast a traffic message to the RSUs to control the traffic light and notify other vehicles that there is an emergency condition.

Due to the VANET has almost fully developed, a lot of value-added service such as vehicle electronic road toll system, traffic control, car location tracking and remote engine diagnosis has been provided by VANET, which enhance driving experience and make drivers more comfortable on the road [2, 3]. However, the traffic related messages in VANET are transmitted by air that has brought up some serious problem in terms of security threats and user privacy [15, 16]. According to the security threats and privacy issue into consideration, our proposed scheme needs to achieve the following security issue [9, 10]:

- Mutual authentication. When receiving the message from a vehicular user, RSU should check whether the user is legal or not. In order to preventing data from tampering, OBU should verify the integrity of transmitted data. On the other hand, when receiving the message from other OBUs or RSUs, a vehicular user also needs to authenticate the validity of other OBUs or RSUs.
- Conditional anonymity. In order to protect vehicular users' privacy, any OBUs or attackers cannot derive the identity of vehicular user from intercepted message. However, if necessary, trust authority (TA) can trace the message source to prevent malicious users.
- Unlinkability. To avoid an attacker collects message form particular vehicle to track its driving route, anyone cannot distinguish the message source from different message package.
- Traceability and revocation. When dispute is happened, TA can trace the user identity from its database, and revoke this user's privileges.

Although many approaches have solved privacy issue in VANET [4, 5, 11, 12, 13], the users still don't know that why access such traffic related message and what personal data is collected. Because the core value of VANET is the traffic related messages, if it doesn't provide a secure VANET environment, users may refuse to submit messages, and it will result in the development of VANET value-added service with a big obstacle. In this paper, our proposed scheme aims to provide better user privacy protection in VANET, which is based on blind signature, more specifically, user can set his/her own privacy preferences and be notified whether his/her privacy preference is suitable for value-added service in VANET environment.

The rest of this paper is organized as follows. In Section 2, we describe some basic preliminaries of our scheme. Our proposed scheme is presented in Section 3. The security analysis of our scheme is given in Section 4. Finally, Section 5 concludes this paper.

2. Preliminaries

As a preliminary, we first introduce the components of VANET. In order to protect user privacy, our scheme is based on privacy coach and blind signature. A brief review of some concepts is provided as follows.

2.1. VANET Environment

Vehicular ad hoc networks (VANETs) are a special case of wireless networks which facilitates vehicles on road to communicate for driving safety [14]. In order to make users feel more comfortable and convenient, more and more value-added service has been provided on road [17]. There are four main components in our scheme, which are provided as follow and the environment of our scheme as shown in Fig. 1:

1) Trust authority (TA): TA is a unit, which is in charge of deployment of RSU and registration of legal vehicles. When there is a traffic incident or other violations, the TA will assist in processing.
2) On-board unit (OBU): OBU is a device in the vehicle, and it has been installed applications, after registering with TA, the OBU will receive the message from the RSU or other vehicle's OBU.
3) RSU (Road Side Unit): RSU is in charge of data exchange between OBU and external Internet. RSU has storage and computational capability. Because the high mobility of vehicles, and the frequent data exchange from one RSU to another; therefore, RSUs have to handle the rapid handoff requirement.
4) Service Provider (SP): In our proposed scheme, SP provides all value-added service such as navigation service, parking service. Moreover, SP is charge of comparing value-added services privacy policy, which is in a fixed XML format, with user privacy preferences. After completing, SP returns result to vehicular user.

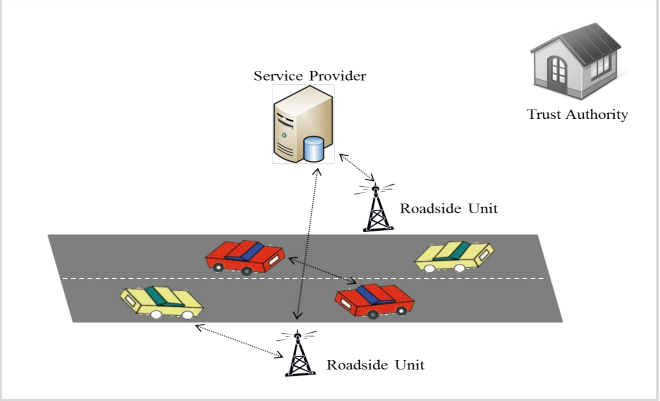

Figure 1. The environment of our scheme

2.2. Privacy Coach

Privacy Coach was proposed by Broenink et al. and the system model of privacy coach is shown in Fig. 2 [6]. Privacy Coach is a mobile application. When users first started using this mobile application, they should fill in a questionnaire. Having finishing, the privacy preferences will be set up, which is result of a questionnaire. Then the user's privacy profile have been stored on the mobile. As user is offered a new RFID tag, just hold its mobile phone to scan the RFID tag, and the coach will ask the provider for offering the privacy policy associated with a tag, which are retrieved from a database. After comparing, the coach tells user whether the corresponding privacy policy fits its privacy profile. The Privacy Coach helps users to determine whether use this RFID tag or not, and users can know more about what personal data will be collected. This software is an open, you can learn more details on [7].We use the concept of Privacy Coach to ensure whether the vehicular users' privacy preference is suitable for value-added service in VANET.

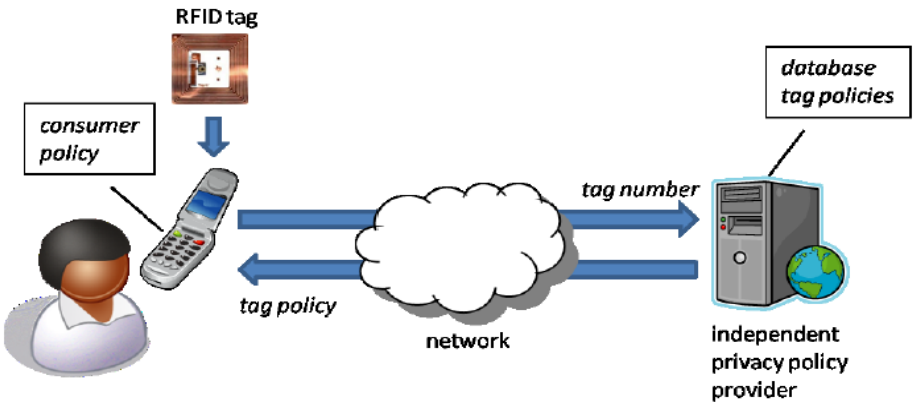

Figure 2. The system model of Broenink et al. 's scheme

2.3. Blind Signature

The concept of Blind Signature was first proposed by David Chaum in 1982[8].It has been used by Li et al. [5], in order to ensure inability to link between vehicle user and service provider. For Blind Signature example, which are two main participant, namely sender and signer respectively, and using RSA algorithm is as follows:

1) The sender first prepares a message m and a random blind factor r, and computes $M = m \times r^e \bmod n$, where (e, n) is a public key of the signer, and send to signer.
2) Upon receiving blind message M sent by the sender, the signer signs the message M with its private key d, and computes $S_M = M^d = m^d \times r \bmod n$.Then the signer send S_M to the sender.
3) Upon receiving the message S_M sent by the signer, the sender can get the signer's signature on the message m by computing $S_m = (m^d \times r) \times r^{-1} \bmod n = m^d \bmod n$.
4) Finally, the others can verify the correctness of S_m by computing $V = {S_m}^e \bmod n$, and check whether $V = m$ or not. The goal of Blind Signature is that verifiers can only verify the correctness of this message's digital signature, but this message can't be traced from whom.

The blind signature technique has the characteristic is namely untraceability that can prevents the signer trace the source of message, and this characteristic is very useful in our scheme for achieving user privacy requirement.

3. Proposed Scheme

In our system, SP may provide various value-added services to vehicular users. In order to let vehicular users know what information is collected and what value-added services is suitable for them, before joining VANET, the vehicular users need to set their privacy preferences by fill in a questionnaire, which is installed in OBU and setup by SP. For example, the question is this service will collect your location information or this service will share your location information with other vehicles, the vehicular user can choose accept or not accept, after finishing, the answer will be recorded and the privacy preferences of the vehicular user will be set up in a fixed XML format and stored on the vehicular user's OBU. An example of a questionnaire is shown in Fig.3.

Privacy Questionnaire

1. **This service will collect your location information**
   □accept □ not accept.
2. **This service will share your location information with other vehicle.**
   □accept □ not accept
3. **This service will provide driving directions to you.**
   □accept □ not accept
4. **This service will trace the status of the car.(e.g. tire pressure).**
   □accept □ not accept
5. **This service will send nearby shops' news.**
   □accept □ not accept

Figure 3. An example of a questionnaire

3.1. System Model

Our proposed scheme for the system model has two phases: request signature phase and comparing phase. In request signature phase, each vehicular user must request a blind signature of his/her privacy preferences from TA. In comparing phase, the vehicular user sends a blind signature and his/her privacy preferences to neighboring RSU.RSU can verify whether the blind signature is legal or not. Once the blind signature is authorized, the RSU sends the vehicular user's privacy preferences to SP. When the vehicular user's privacy preferences are received, the SP compare user's privacy preferences with value-added services privacy policy, which is provided by SP. SP will check each variable of policies, then provides appropriate value-added services to vehicular user, and allow RSU to collect driving related data from vehicular user. Fig. 2 shows our system model.

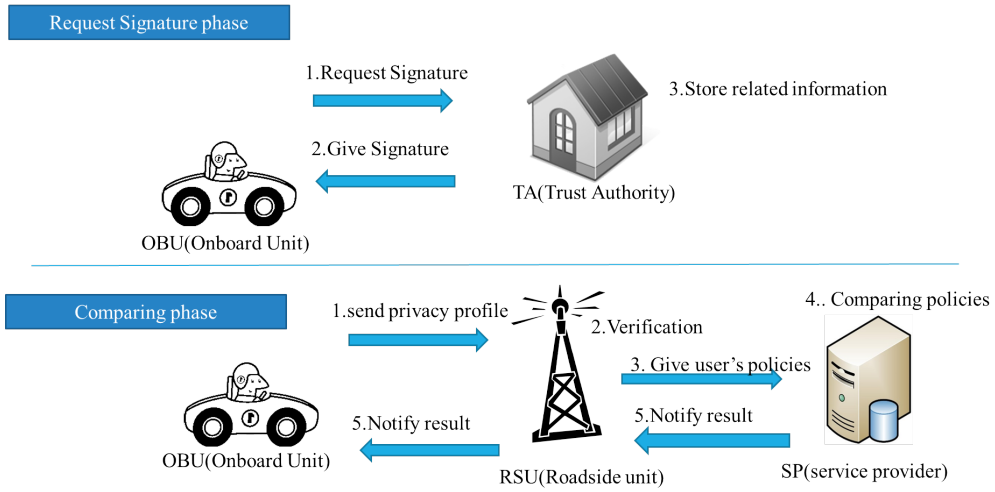

Figure 4. System model of our scheme

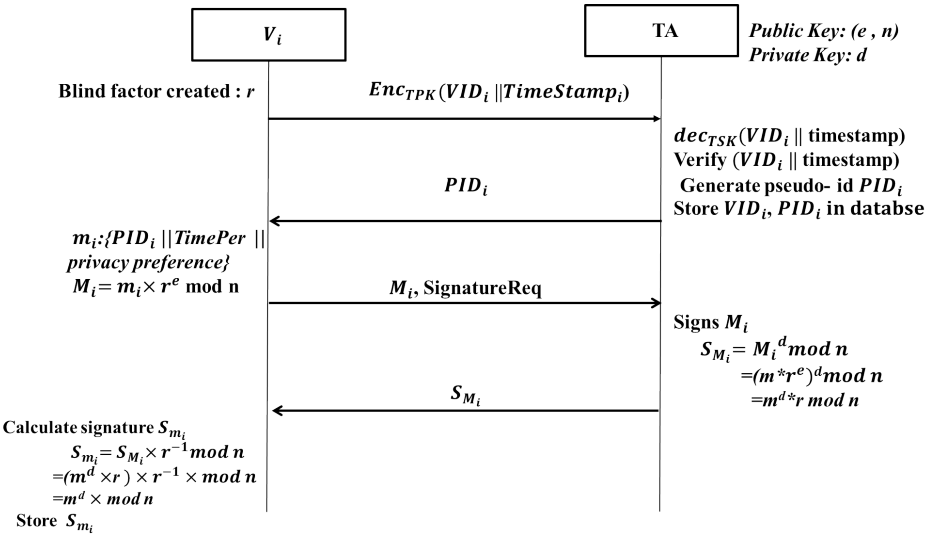

Figure 5. Request Signature Phase

3.2. System Parameters

Table 1. Notations used through the proposed scheme

VID_i	A real identity of vehicular user i.
PID_i	A pseudo identity of vehicular user i.
$Enc_x(m)$	The asymmetric encryption function with x Key
$Dec_x(m)$	The asymmetric decryption function with x Key
$TimeStamp_i$	A timestamp, which vehicular user i attached.
$TimePer$	TimePer is time period, which represents the user privacy preferences period. For example, if user want to use this privacy preferences during 12:00 PM to 5:00 PM, the TimePer is 1200PM0500PM.
m_i	It includes PID_i, TimePer , privacy preferences
S_m	The signature of message m.
RID_i	The identity of RSU i
RL_i	The location of RSU i
RC_i	The certificate of RSU i
TPK	The public key of TA
TSK	The secret key of TA
$SIG_{TSK}(m)$	TA's signature on message m by using TSK

The notation used in the rest of this paper is shown in Table 1.

3.3. Initial Phase

In the initial phase, TA assigns itself a pair of public key and secret key, TPK and TSK. TA publishes its public key TPK. TA also deploys each RSU R_i located at RL_i and assigns each RSU R_i an identity RID_i. TA then generates R_i's certificate as $RC_i = SIG_{TSK}(RID_i, RL_i)$, and each R_i will store RID_i, RL_i and RC_i.

3.4. Request Signature Phase

In request signature phase, there are two main participants, namely vehicular user and TA respectively; a vehicular user wants to obtain the blind signature of his/her privacy preferences. After receiving user's real identity and privacy preferences from vehicular user, TA generates pseudo identity and blind signature of privacy preferences to vehicular user. The procedure and following step are shown in Fig. 5.

1. The vehicular user V_i first encrypts (VID_i $||Timestamp_i$) by using TA's public key and sends to TA, where VID_i is real identity of vehicular user and $Timestamp_i$ is generated by V_i.
2. After receiving $Enc_{TPK}(VID_i||Timestamp_i)$ from V_i, TA decrypts it by using his private key, and verifies the validity of $Timestamp_i$, if $Timestamp_i$ is not valid, the procedure will be cancelled; otherwise, TA generates a corresponding pseudo-id PID_i, storing VID_i and PID_i in the TA's database. Then TA sends PID_i back to V_i.
3. Frist V_i can specify the $TimePer$, then concatenate his/her pseudo identity PID_i, $TimePer$, $privacy\ preferences$ as m_i, which is the result of privacy questionnaire, and select blind factor r to computing $M_i = m_i \times r^e mod\ n$,where (e, n) is TA's public key. At lest V_i send M_i and request signature message $SignatureReq$ to TA.
4. Upon receiving M_i, TA signs M_i with its private key d, by computing $S_{M_i} = {M_i}^d mod\ n = (m_i \times r^e)^d mod\ n = m^d \times r\ mod\ n$, then send back to V_i.
5. After receiving S_{M_i} from TA, V_i can obtain the signature S_{m_i} on message m_i, by computing $S_{m_i} = S_{M_i} \times r^{-1}\ mod\ n = ({m_i}^d \times r) \times r^{-1}\ mod\ n = {m_i}^d\ mod\ n$. V_i can confirm the correctness of S_{m_i} by checking whether ${S_{m_i}}^e\ mod\ n = m_i$ or not. If verification is successful, store m_i and the blind signature S_{m_i}; otherwise, drop it and the procedure will be cancelled.

3.5. Comparing Phase

In comparing phase, there are three main participants, namely vehicular user V_i, RSU, and SP respectively. The vehicular user request to know which value-added services is suitable for his/her privacy preference. RSU is in charge of verifying correctness of the S_{m_i}, and SP are responsible to compare the user's privacy preferences with value-added services privacy policy. The procedure and following step are shown in Fig. 4.

1. The V_i will send m_i :{ PID_i, $TimePer$, $privacy\ preferences$} and S_{m_i} to neighbor RSU.
2. Upon receiving m_i and S_{m_i}, the RSU verifies whether ${S_{m_i}}^e\ mod\ n = m_i$ or not, where (e, n) is TA's public key. If verification is successful, the RSU can convinced that m_i is a legal message rather than a forgeable message, then the RSU send m_i, its identity RID_i, its location RL_i, its certificate RC_i and request comparing message $ComparingReq$ to SP.
3. First, SP uses TA's public key TPK to verify whether $Dec_{TPK}(SIG_{TSK}(RID_i||RL_i)) = (RID_i||RL_i)$ or not, if verification is successful, SP can ensure this RSU is a legal unit. If this RSU is an illegal unit, SP will notify TA. Then, SP check whether $TimePer$ is valid or not, if $TimePer$ has expired, the following steps are stopped; otherwise, the SP will start to compare V_i 's $privacy\ preferences$ with value-added services privacy policy, where value-added services privacy policy is provided by the SP, SP will compare each variable of policy with vehicular user's privacy preferences
4. According to the results of comparison, SP allows the RSU to collect traffic related messages from V_i, and provides the suitable value-added services for vehicular users ,then RSU sends its identity RID_i, its location RL_i, its certificate RC_i and notifies V_i what information RSU collected and how to use. However, if all variables are not matched, the SP doesn't allow RSU to collect any information from V_i, and informs V_i that your privacy preferences are not suitable for any value-added services and the RSU will not collect your any message.
5. After receiving message and RID_i, RL_i, RC_i from RSU, V_i uses TA's public key TSK to check whether $Dec_{TPK}(SIG_{TSK}(RID_i||RL_i)) = (RID_i||RL_i)$ or not, if verification is successful, V_i can ensure the message that the RSU notified is valid, and believe that his/her privacy is protected.

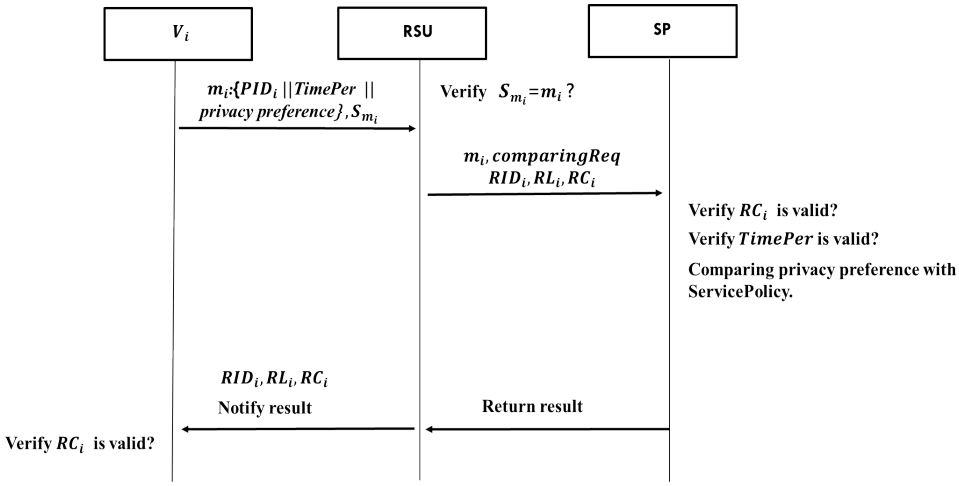

Figure 6. Comparing Phase

4. Security Analysis

In this section, we will demonstrate security requirements that mention in section 1 of the proposed scheme.

4.1. Mutual Authentication

In comparing phase, the vehicular user needs to send m_i and blind signature S_{m_i} to nearby RSU, after receiving that from the vehicular user, RSU can check whether ${S_{m_i}}^e \bmod n$ is equal to m_i by using TA's public key. If so, RSU can believe that the vehicular user holds authentication message m_i and blind signature S_m. Moreover, the vehicular user also needs to check whether $RC_i = SIG_{TSK}(RID_i||RL_i)$ is equal to $(RID_i||RL_i)$ by using TA's public key. If so, the vehicular user can convince that this RSU is a legal unit. Since TSK is only known by TA, no one can forge the signature that TA signed, our purposed scheme achieves mutual authentication and resists RSU replication attack. The most important is this security requirement protects our scheme from malicious units or users.

4.2. Conditional Anonymity

In this section, we will illustrate that real identity of a vehicular user cannot be exposed easily. In request signature phase, the vehicular user encrypts his/her real identity by using TA's public key and sends it to TA. Because only TA can decrypts it by using its secret key, the vehicular user's real identity cannot be known by others. After receiving it from the vehicular user, TA generates a corresponding pseudo identity PID_i, and then sends back to the vehicular user. After that, the vehicular user communicates with each other by using pseudo identity. As a result, no one can expose real identity of the vehicular user except TA, and our purposed scheme achieves conditional anonymity.

4.3. Unlinkability

In this section, we show that why TA or RSU cannot link up a vehicular user's real identity easily. In request signature phase, the vehicular user send message M_i and request blind signature from TA, TA signs M_i and send S_{M_i} to the vehicular user. The vehicular user can obtain S_{m_i}. Even if TA cannot know the source of m_i, because m_i is not equal to M_i that TA has signed. As a result, TA unable to trace the source of m_i, and our proposed scheme satisfies unlinkability.

4.4. Traceability and Revocability

If the RSU or SP finds that V_i is a malicious user, it will report to TA. TA can use PID_i to search its database and find out corresponding VID_i, and then trace this vehicular user and revoke his/her right to our purposed scheme. Therefore, our proposed scheme can meet traceability and revocability; it's very helpful for our proposed scheme to resist malicious users.

5. Conclusions

We proposed a novel protocol for the value-added services in the VANET environment, which based on blind signature technology, and is very useful to solve information asymmetry between the vehicle user and data collector. Different from other method, our proposed scheme lets user can set up his/her privacy preference, which is compared with value-added services privacy policy, and provides appropriate value-added services service for the users. Hence, the user can know that how traffic related message about her/him be used and what personal data is collected. In addition, in our proposed

scheme, the vehicular users utilized pseudo identity to communicate with other units, and it can protect the vehicular user's privacy. Moreover, with the blind signature technology, no one including TA cannot link up the source of message and user's identity. With the rapid of smart devices, there are more and more value-added services are provided. As a result, protect user's privacy is more and more important. Our proposed scheme is suitable for value-added services in VANET environment and very helpful for developing of Intelligent Transportation System and Smart city.

REFERENCES

[1] Theodoridis, E., Mylonas, G., & Chatzigiannakis, I. (2013, July). Developing an IoT Smart City framework. In Information, Intelligence, Systems and Applications (IISA), 2013 Fourth International Conference on (pp. 1-6). IEEE.

[2] Zhao, Y. (2002). Telematics: safe and fun driving. IEEE Intelligent Systems, 17(1), 10-14.

[3] He, W., Yan, G., & Xu, L. (2014). Developing vehicular data cloud services in the IoT environment.

[4] Xiong, H., Zhu, G., Chen, Z., & Li, F. (2013). Efficient communication scheme with confidentiality and privacy for vehicular networks. Computers & Electrical Engineering, 39(6), 1717-1725.

[5] Li, C. T., Hwang, M. S., & Chu, Y. P. (2008). A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. Computer Communications, 31(12), 2803-2814.

[6] Broenink, G., Hoepman, J. H., Hof, C. V. T., Van Kranenburg, R., Smits, D., & Wisman, T. (2010). The privacy coach: Supporting customer privacy in the internet of things. arXiv preprint arXiv:1001.4459.

[7] Dutch interdisciplinary forum on RFID,http://www.difr.nl/

[8] Chaum, D. L. (1988). U.S. Patent No. 4,759,063. Washington, DC: U.S. Patent and Trademark Office.

[9] Raya, M., Jungels, D., Papadimitratos, P., Aad, I., & Hubaux, J. P. (2006). Certificate revocation in vehicular networks. Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL, Switzerland.

[10] Studer, A., Shi, E., Bai, F., & Perrig, A. (2009, June). TACKing together efficient authentication, revocation, and privacy in VANETs. In Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on (pp. 1-9). IEEE.

[11] Hyoung-Kee, C., In-Hwan, K., & Jae-Chern, Y. (2010). Secure and efficient protocol for vehicular ad hoc network with privacy preservation. EURASIP Journal on Wireless Communications and Networking, 2011.

[12] Xiong, H., Zhu, G., Chen, Z., & Li, F. (2013). Efficient communication scheme with confidentiality and privacy for vehicular networks. *Computers & Electrical Engineering*, *39*(6), 1717-1725.

[13] Lu, R., Lin, X., Zhu, H., Ho, P. H., & Shen, X. (2008, April). ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE.

[14] Raya, M., & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. Journal of Computer Security, 15(1), 39-68.

[15] Dötzer, F. (2006, January). Privacy issues in vehicular ad hoc networks. In Privacy enhancing technologies (pp. 197-209). Springer Berlin Heidelberg.

[16] Yousefi, S., Mousavi, M. S., & Fathy, M. (2006, June). Vehicular ad hoc networks (VANETs): challenges and perspectives. In ITS Telecommunications Proceedings, 2006 6th International Conference on (pp. 761-766). IEEE.

[17] Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., & Zedan, H. (2014). A comprehensive survey on vehicular Ad Hoc network. Journal of network and computer applications, 37, 380-392.

[18] Yang, Y., & Bagrodia, R. (2009, September). Evaluation of VANET-based advanced intelligent transportation systems. In Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking (pp. 3-12). ACM.