Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.4, Aug. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.4.941

이동 중인 전기자동차 무선충전의 보안위협 분석*

제이납 리자이파,† 오 희 국‡
한양대학교 컴퓨터공학과

Analysis of Security Issues in Wireless Charging of Electric Vehicles on the Move*

Zeinab Rezeifar,† Heekuck Oh‡
Department of Computer Science and Engineering, Hanyang University

요 약

화석 연료의 사용이 문제가 되고 있는 상황에서, 고효율 전기 엔진의 등장은 전기 자동차 개발을 가속화시켰다. 하지만 전기 자동차의 개발 비용을 줄이기 위해 소형 베터리를 사용한 결과 충전 빈도가 잦아져 불편을 유발하게 되었다. 이동식 무선충전 기술이 해결책으로서 활용될 수 있지만, 충전의 빈도가 잦아지면 사용자의 위치정보를 노출하게 되는 문제점이 존재한다. 본 논문에서는 전기 자동차의 무선충전 기반시설을 제안하고, 이때 발생할 수 있는 보안이슈에 대해 분석한다.

ABSTRACT

Limitation of fossil energy from one side and the efficiency of the electrical engine from another side motivate the industrials to encourage people for utilizing electric vehicles (EVs). To decrease the cost of EVs, the size of battery should be reduced which causes an inconvenient frequent recharging. Wireless charging is a solution for charging of electric vehicles on the move, but frequent charging causes to disclose users' location information. In this paper, we first propose an infrastructure for wireless charging of electric vehicles, and then we explain security issues that can be stated in this condition.

Keywords: Electric Vehicles, Infrastructure, Location information, Security issues

I. Introduction

With improving the industry and increasing the number of combustion engines, environmental pollution and energy crisis are a serious problem that world faces which can be alleviated by using Electric Vehicles (EVs) [1]. However, the most significant reason of selecting EVs for replacement of combustion engine is the efficiency of its engine in using electrical power. The combustion engine can only use about 30% of fuel of its fuel tank, and the most of its energy wastes in heating While the efficiency of the electrical engines are more than 80% which is an important reason for introducing Plug-in Electric Vehicle (PEV). However, to commercialize

Received(03. 23. 2016), Modified(08. 03. 2016), Accepted(08. 05. 2016)
* 이 논문은 2015년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2015R1D1A1A09058200)
* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2016-H8501-16-1018)
† 주저자, rezaeifar@hanyang.ac.kr
‡ 교신저자, hkoh@hanyang.ac.kr(Corresponding author)

EVs, the price and the size of the battery, which are main reasons to prevent electrical power being the main source for the vehicles, should be reduced. Despite the fact that combustion vehicle can move more than 500 km without refueling, an electrical battery has an average driving 120km [2]. Also, this limitation of driving accompanies with the lack of charging places. Moreover, to achieve longest duration of usage power by increasing size of battery, it rises the price of EVs significantly.

To counter the above problems of PEVs, wireless charging technology has been introduced. By charging on the move, the number of times that a driver needs to stop for recharging will decrease, which makes it more comfortable for the users. In this case, the industry can decrease the size of the battery, reducing the price of EVs and making them more commercial [3]. The On-Line Electric Vehicle (OLEV) project, which has been recently carried out by the Korea Advanced Institute of Science and Technology (KAIST), was selected as one of the best innovations of 2010 [4]. In this project, electric vehicles can be charged remotely from power transmitters that are installed under the road, so EVs can be charged when they move on the road, and the recharging downtime is significantly reduced. Also, this project has achieved the power transfer efficiency of 80% with an air gap of 10 cm between an underground coil and a power receiving unit in the vehicle [3].

In the best of our knowledge, although OLEV project is successful for reaching significant efficiency and decreasing downtime for charging, there is no an infrastructure defined for communication between a charging place and vehicles which consider security issues during exchanging of information and paying the bill for charging. Due to these drawbacks, this project has not been widely adopted.

Contribution: Since wireless charging has an important effect on reaching significant efficiency and reducing downtime for recharging, in this paper, we first propose an infrastructure for wireless charging EVs on the move. Then, we mention security issues that may offer in these communications since considering security issues make this innovation more practical.

The rest of the paper is organized as follows. We mention related work regarding wireless charging of EVs in section II. In section III, we discuss our proposed infrastructure for wireless charging. In section IV, we present the security issues in wireless charging. Finally, some conclusions and future works are given in section V.

II. Related Work

A typical Vehicular Ad-hoc NETwork (VANET) consists of vehicles, a Road Side Unit (RSU) as an access point and a collection of location servers. The vehicles use an on-board communication unit to exchange messages between each other and an RSU. Moreover, vehicles are equipped with sensors and data units to collect environmental information such as vehicle speed, vehicle locations and etc. The RSU sends the information to the location servers through wired communication. All the information from an RSU is recorded in the service provider to process accompany with other information from different data sources such as traffic management system, weather information system and etc. Moreover, the location servers connect to

different Service Provider (SP) to provide various location based services for vehicles. Furthermore, a trusted Registration Authority (RA) provides authentication for both service providers and vehicles [4].

The interaction between intelligent vehicles and the power grid can be used in multiple dimensions. In the Intelligent Transportation System (ITS), the Smart Grid (SG) concept is considered in mid-2011. The interface between SG and ITS consists of vehicle charging units to exchange electricity power to users. Moreover, to facilitate charging on the move, EVs should interact with road, energy and communication infrastructure, so intelligent vehicles should communicate with SG to optimize transportation related tasks [5]. The Current operation in the SG is based on field sensors to obtain a measurement from distribution infrastructures which connect to the power grid through the wire. However, the smart grid applications need far more measurement from the grid which can improve with wireless communication and micro-electro-mechanical systems to enable the new kind of wireless sensing technology which is integrated with data processing and communication components.

The nature of wireless device not only decreases the price of infrastructure but also is suitable to gather fine-grained measurement required by the smart grid applications [6]. Moreover, on-board chargers require cable and plug-in charger, but Wireless Power Transfer (WPT) provides charging conductively to address these problems. Indeed, inductive charging works by separating two halves of the inductive coupling interface which are primary and secondary of a two-part transformer [7].

In the OLVE project, the battery is charged remotely from the power transmitter installed under the road. Wireless power pickup device is installed under the cars to remotely collect power from underground power transmitter automatically. When the power transmitter is constructed on the road, the road is divided into multiple zones to select the best place for installing power transmitters. The power transmitter consists of the inverter and the inductive power cable. The length of inductive cable depends on the power requirement of the vehicle. The major cost of automated charging is the cost of battery and the power transmitter which consists inverters and inductive cables [8].

To the best of our knowledge, there is no research paper regarding security issues in wireless charging of EVs on the move. To discuss the security issues in this area, we first suggest an infrastructure for charging EVs on the move. Therefore, we classify security issues in two parts regarding communications, namely, Vehicle to Grid (V2G) and Vehicle to Power plate (V2P). In the following sections, we disclose security issues in these two parts.

III. Proposed Infrastructure

In this section, we mention the infrastructure that can be used for wireless charging of the electric vehicles. As illustrated in Fig.1, data dissemination in wireless charging of electric vehicle can be based on three communication parts as follows:

◉ *Vehicle to Grid (V2G)*: Vehicle can connect to the grid through VANET and uses an RSU with Dedicated Short

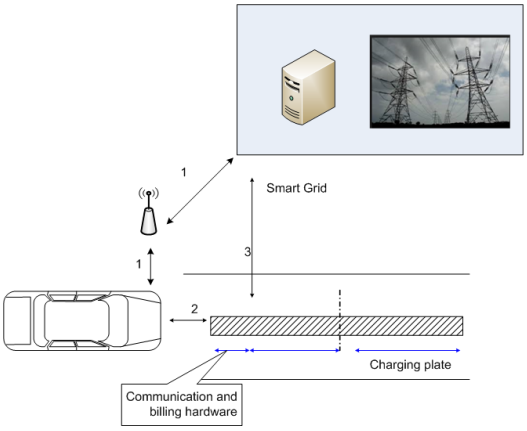

Fig. 1. Infrastructure of wireless charging of electric vehicle

Range Communication (DSRC) capabilities of vehicles. We assume vehicles are equipped with an On Board Unit (OBU).

◉ *Vehicle to Power plate (V2P) and Power plate to Vehicle (P2V)*: Vehicles can connect to power station plate installed under the ground wirelessly.

◉ *Power plate to Grid (P2G)*: Power station plates are connected to the grid through the high-speed wired links.

3.1 V2G communication

We assume that grid contains power transmission units for transferring electrical energy to the power station plates. Also, it contains a central controller that manages the actual charging decision of EVs. This system can give information such as the cost of each charging plate.

First, vehicles send a request to the grid through an RSU, and the RSU sends this request to the grid. After authentication of the request, the grid offers different charging plates which are nearest to the position of this vehicle.

Then, the vehicles can find the best

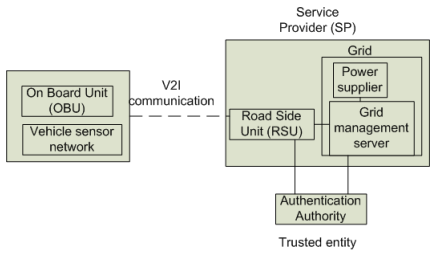

Fig. 2. Vehicle to the grid communication

place for charging based on their destination and the cost of charging. As shown in Fig.2, the RSU is connected to the grid through the wired network. Furthermore, the trusted registration authority (RA) provides authentication and the authorization service for both electric vehicles and the grid which is shown in Fig.2.

3.2 V2P communication

The charging plate consists of two parts, one for communication with vehicles for the charging bill and another part is the charging plate. Moreover, the charging plate is segmented into the specified parts to give defined charge to the vehicles as shown in Fig.3.

First, the electric vehicle sends the amount of the charging request to the plate which is defined by a vehicle sensor device. After authentication, it gives the validation to use the number of charging

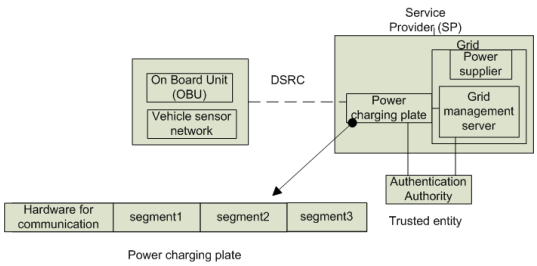

Fig. 3. communication between vehicle and charging plate

segmentations according to the user's request.

Since the distance between vehicles and a charging plate is so short, we assume Near Field Communication (NFC) protocol for communicating between EVs and a charging plate. NFC is communication protocols that enable two electric devices, one of which is usually a portable device to establish communication in the short range of each other. With applying NFC protocols, we reduce DoS and eavesdropping attacks which is a significant problem in wireless communication with a large range.

3.3 P2G communication

The power station connects to the grid to give information about the charging price for disturbing energy. Also, it can connect to the trusted party for the authentication process. Although in current technology, charging station connects to the server through the wire, to improve communication, which has been explained in related works, the charging plate should communicate with the SG wirelessly.

IV. Security Issues

In this section, we mention security issues that can be considered in wireless charging of EVs. According to our proposed infrastructure, we can discuss security issues in two parts. In the first part which is related to the communication of vehicles with SG via VANET, the security problems are same as in VANET for accessing location-based service applications. In the second part, for connecting EVs to charging plate, the security issues related to charging can be considered. Table 1 shows the brief comparison between two communication parts. Using NFC protocols in V2P prevents DoS and eavesdropping attacks in this communication. In the following, we explain each part more.

4.1 Security Issues in Vehicle to Grid Communication

VANET is the subset of the Mobile Ad-hoc Network (MANET) in which the nearby vehicles and RSUs can communicate with each other. In VANET, vehicles are equipped with an OBU, so there are two kinds of nodes namely, an OBU and an RSU. The OBU is installed in vehicles while the RSU is infrastructure mounted along the road which acts as an intermittent node to provide communication between vehicles or a vehicle and the grid [9]. Recently security

Table 1. Comparison security and privacy attacks in V2G and V2P communication parts

security and privacy attacks	V2G	V2P
Dos attacks	√	×
Eavesdropping	√	×
Impersonation	√	√
Message alteration	√	√
Message delay	√	×
Hardware tampering	√	√
location privacy	√	√

issues in VANET are considered as a challenging topic. In [10], the various security and privacy issues in VANET are stated. Moreover, there are some features that make VANET more challengeable which are mentioned as follows [11]:

- *Time constraints*: One of the significant factor in VANET is the limitation of time. The message should be sent in the specific time especially for the safety applications that they have a deadline and after that, the messages will not be accepted.
- *The scale of the network*: VANET is one of the largest networks in which the number of nodes exceeds 750 million, and it is still increasing too, so a global authority needs to govern this huge network.
- *The high mobility of nodes*: The high mobility of nodes in VANET causes to apply specific authentication techniques that are fast and does not need a handshake in which all of the nodes communicate only once.

Despite these challenges, there are many applications that motive researchers to improve security issues in this network. Applications can be classified into three groups namely, cooperative driving, probe vehicle data, and Location Based Service (LBS). In the cooperative driving, which is based on Vehicle to Vehicle (V2V) communication, vehicles broadcast a safety message contained e.g. their speed, locations and velocities every 500 ms to improve safety and coordination of vehicles for refining the control traffic.

The probe vehicle data is based on Vehicle to Infrastructure (V2I) communication in which the RSU collects traffic condition information from vehicles equipped with short range radio e.g. DSRC or long range communication devices e.g. cellular network to monitor the road. The RSU sends probe data requests in its range, and the vehicles in this range will reply these messages. The interval for sending a replying message to the probe data request depends on the application requirement. For example, when the probe car volume is one vehicle per minute for the real-time congestion estimation, the broadcast interval of data should be 3 minutes [4].

The LBS applications use vehicles' location to give the appropriate service for users' requests e.g. querying about the closest shopping mall to its current location. Furthermore, in the proposed infrastructure for wireless charging of EVs on the move since vehicles at first step should connect to the grid through an RSU to receive information of the nearest wireless charging in their paths. This request can be also considered as the location-based service application in VANET.

4.1.1 Security Threats

VANET like other networks encounters different kinds of attacks. However, we can classify the intentions of these attacks as below [12]:

- *Confidentiality*, such as collecting valuable data from users which are exchanging between vehicles or vehicles and infrastructures.
- *Integrity*, such as alerting, deleting or modifying of the exchanging messages especially for V2V communications compare to V2I because of their fragility.
- *Availability*, such as Denial of Services

(DoS) attacks which use resources, services and applications.

In general, VANET's threats can be categorized as follows [11]:

◉ *DoS attacks*: This kind of attacks try to block the communication and interrupt the services.
◉ *Eavesdropping*: The goal of this attack is to achieve the confidential information which can be prevented with the encrypted data.
◉ *Impersonation*: In this attack, the malicious node uses someone else's identity to pretend to be another user. For example, with this attack, an innocent user might be arrested in the case of an accident. Digital signature and certification can prevent impersonation, alteration and illegal injection of packets to the network.
◉ *Message alteration*: This attack happens to change information passed through nodes or provides fake information. For example, a malicious node pretends that an accident happens ahead but actually this is not the case.
◉ *Message delay*: This refers to the case when a malicious node holds on the message before forwarding it. It is a critical situation for the safety applications in which delay is a significant role.
◉ *Hardware tampering*: This attack happens at the manufacturing level to manipulate node physically.

However, vehicle communications with the smart gird for getting information of the nearest charging plate are similar to location-based service applications in VANET, so the privacy threat is a significant attack that should be considered in these applications. In the privacy threat, the adversary tries to associate the identity of users with the users' private information. Moreover, the private information and the identity of users can be achieved by users' requests to the service provider or with the available background knowledge. In the [13], the attacks enabled by the background knowledge are classified as bellow:

◉ *Attacks exploiting quasi-identifiers*: In this attack, the private information can be gained by joining data in the request message with external information. For example, if the location information is mentioned in the request message, we can recognize the identity of the individual with the public available present data. In this case, the location data acts as quasi-identifier.
◉ *Snapshot versus Historical attacks*: In the snapshot attack, only one message at the given instant is considered while in the historical attack, the adversary can link a set of requests.
◉ *Single versus Multiple-Issuer Attacks*: If the adversary model is related to the request from one user, it is a single issuer attack. Otherwise, if it is related to multiple requests from different users, it will be called multi-issuer attacks. Moreover, in multi-issuer attacks, the adversary can access sensitive associations for a user although they cannot identify the user.

4.1.2 Defense to LBS applications threats

Defense techniques can be classified according to the attacks, but they can also be categorized according to other features such as follows [13]:

Table 2. Requirements for the secure payment methods in plug-in charging versus wireless charging on the move

requirement	Plug-in charging	wireless charging on the move
Time constraint	×	√
Anonymity	√	√
Track illegal users	√	√

◉ *Identity anonymity versus private information obfuscation*: Anonymity methods provide users' anonymity to protect association between private information and the identity of users. Using different pseudonym to hide the real identity of users can be considered as these kinds of defenses, while the goal of private information obfuscation methods is to hide the individual private information among general requests.

◉ *Centralized versus decentralized defense*: The centralized defenses assume one or more trusted entities between the service provider and users. These trusted entities act as a proxy to provide privacy of issuers whereas decentralized methods do not consider an entity between service provider and issuers.

For location-based service applications in VANET, users may ask for the closest shopping mall, restaurants to their locations that V2I and V2V communication can be utilized by an adversary to access network identifiers and the location estimation of the communication vehicles. In [14], to reduce the profiling of LBS application accessed by a target vehicle, the target location is distorted in temporal and/or spatial dimensions. Also, the authors use the group concept that vehicles can send a request to the service provider anonymously by using a group leader as a proxy. In [4], in order to prevent trace back of the LBS request broadcasted in the group concept, the authors use group leader as MIX [15] which hides the correspondence between items in its input and those in its output with changing the appearance and order of inputs due to mixing . In this method, the group leader first decrypts the message received from one vehicle in the group to change appearance and waits for more LBS requests from at least one another member in the group. Then, the bundle of requests is forwarded to the RSU in random order. Therefore, the adversary cannot identify the LBS requests from one vehicle by correlating the appearance of that vehicle to the group leader and from the group leader to the RSU.

4.2 Security Issues in Vehicle to charging Plate communication

For wireless charging EVs, secure communication is required between EVs and a charging plate which should happen at a very high rate. The IEEE 802.11 p standard suggests the use of Elliptic Curve Digital Signature Algorithm for authentication in VANET, but this method takes a significant amount of time to sign and verify the signature. In [16], the authors consider the power grid as a trusted entity. As EVs need to authenticate during charging from the charging plate, they use pseudonyms

which only the smart grid can map it to the identity of the real vehicle. Moreover, vehicles should change pseudonyms with connecting to the smart grid after each charging. However, if the service provider receives pseudonym and does not give charge, users can not do anything.

In [17], the authors propose a fast authentication method for wireless charging of EVs. In this method, the neighbor RSUs share the same secret key for communication between an RSU and EVs, so it will avoid re-key re-establishment between EVs and neighbor RSUs. Therefore, this method allow the EV to communicate with all subsequent RSUs along its path with the same key. However, in this method, the EV cannot directly communicate with the charging plate, and it should communicate with charging plate through an RSU. Moreover, this method does not provide location privacy which is the main security problem in wireless charging of EVs on the move.

Most of EVs can go about 120 km before recharging which needs to recharge frequently in a day. This may disclose the user's private information such as location and interested places of vehicle users. Moreover, the location information can be misused for crimes such as kidnapping or automobile thefts, so providing location privacy is a significant issue in this condition. However, as shown in Table 2, there are different requirements for secure payment methods of wireless charging on the move versus plug-in charging. One of the most important features that should be kept in our mind for wireless charging on the move is time and the fast operation payment system as vehicles have considerable speed while it is not a requirement for plug-in charging. However, since an EV needs to charge frequently in a day, the location privacy of the EV can be abused to profile the owners of the EV, so anonymity should be considered in payment method to protect users' location privacy in the both plug-in charging and wireless charging on the move. Moreover, with users' consent, the transaction should be traceable and a trusted party should be able to revoke the illegal users from the system in both charging systems.

In the [18], the authors propose a new payment system for enhancing location privacy in electronic vehicles. In this method, the authors suppose that vehicles equip with in-car-unit consists of small read-only memory which will be initialized during the registration process. During the registration process, the user should contact the supplier for opening an account and paying a deposit for at least D dollars which are the amount needed for paying the requested charge service. In charging process, the in-car-unit carries an interactive protocol to communicate with the charging plate, and it also communicates with the supplier to check the balance of user anonymously. At every statement, users should approach the supplier to increase their balance to make it D dollars again. Moreover, with user's consent, the judge can trace all transactions conducted by this user. However, in this paper, the authors used bilinear pairing and zero knowledge proof for verifying users account to the service provider in which only the charging process takes 10 seconds that will not be appropriate for wireless charging when vehicles move on the road.

However, with the proposed infrastructure for wireless charging on the move, we reveal that one of the

challenging security issues is providing privacy which can be threatened during paying. As a part of future work, we want to propose a light anonymous method to protect location privacy for this infrastructure.

V. Conclusion and Future Work

Wireless charging makes EVs more convenient and cost efficiency which can accelerate the replacing of electric vehicles with combustion engines. Therefore, in this paper, we have suggested the infrastructure for wireless charging of electric vehicles on the move. Besides, we have explained security problems in this infrastructure. One of the most significant security problem in the wireless charging on the move is location privacy as electric vehicles needs to charge frequently in a day, so finding a secure solution for paying and connecting vehicles to the power stations without any leak of information of users is challenging in this area. Although some methods for location privacy in VANET and location privacy in plug-in EVs were proposed but none of them were appropriate for wireless charging of electric vehicles. Therefore, as a part of our future work, we intend to find a proper solution for location privacy in wireless charging of electric vehicles on the move.

References

[1] T.R. Hawkins, B. Singh, G. Majeau-Bettez, and A.H. Stromman, "Comparative environmental life cycle assessment of conventional and electric vehicles," Journal of Industrial Ecology, vol. 17, no. 1, pp. 53-64, Oct. 2013.

[2] P. Dutta, "Coordinating rendezvous points for inductive power transfer between electric vehicles to increase effective driving distance," Proceedings of the International Conference on Connected Vehicles and Expo (ICCVE), pp. 649-653, Dec. 2013.

[3] N.P. Suh, D.H. Cho, and C.T. Rim, "Design of on-line electric vehicle (OLEV)," Proceedings of the 20th CIRP Design Conference, pp. 3-8, Feb. 2011.

[4] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for vanet," IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1569-1589, Oct. 2007.

[5] X. Cheng, X. Hu, L. Yang, I. Husain, K. Inoue, P. Krein, R. Lefevre, Y. Li, H. Nishi, J.G. Taiber, F.Y. Wang, Y. Zha, W. Gao, and Z. Li, "Electrified vehicles and the smart grid: the ITS perspective," IEEE Transactions on Intelligent Transportation Systems, vol. 15, no. 4, pp. 1388-1404, Aug. 2014.

[6] F. Bouhafs, M. Mackay, and M. Merabti, "Overview of the Smart Grid," Communication Challenges and Solutions in the Smart Grid, SpringerBriefs in Computer Science, pp. 1-12, Nov. 2014.

[7] F. Musavi, M. Edington, and W. Eberle, "Wireless power transfer: A survey of EV battery charging technologies," Proceedings of the IEEE Conference in Energy Conversion Congress and Exposition (ECCE), pp. 1804-1810, Sep. 2012.

[8] Y.D. Ko, Y.J. Jang, and S. Jeong, "Mathematical modeling and optimization of the automated wireless charging electric transportation system," Proceedings of the IEEE International Conference on Automation Science and Engineering (CASE), pp. 250-255, Aug.

2012.
〔9〕 M.N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," Vehicular Communications, vol. 1, no. 2, pp. 53-66, Apr. 2014.
〔10〕 M.E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," Proceedings of the European Wireless Workshop, pp. 270-274, Feb. 2002.
〔11〕 R.G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," Computer Communications, vol. 44, pp. 1-13, May 2014.
〔12〕 G. Yan, D. Wen, S. Olariu, and M.C. Weigle, "Security challenges in vehicular cloud computing," IEEE Transactions on Intelligent Transportation Systems, vol. 14, no. 1, pp. 284-294, Sep. 2013.
〔13〕 C. Bettini, S. Mascetti, X.S. Wang, D. Freni, and S. Jajodia, "Anonymity and historical-anonymity in location-based services," Privacy in Location-Based Applications, LNCS 5599, pp. 1-30, 2009.
〔14〕 M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," Proceedings of the ACM International Conference on Mobile Systems (MobiSys), pp. 31-42, May. 2003.
〔15〕 D.L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 24, no. 2, pp. 84-90, Feb. 1981.
〔16〕 H. Nicanfar, S. Hosseininezhad, P. Talebifard, and C.M. Leung, "Robust privacy-preserving authentication scheme for communication between electric vehicle as power energy storage and power stations," Proceedings of the IEEE INFOCOM, pp. 3429-3434, Apr. 2013.
〔17〕 H. Li, G. Dan, and K. Nahrstedt, "Proactive key dissemination-based fast authentication for in-motion inductive EV charging," Proceedings of the IEEE International Conference on Communications (ICC), pp. 795-801, June 2015.
〔18〕 M.H. Au, J.K. Liu, J. Fang, Z.L. Jiang, W. Susilo, and J. Zhou, "A New Payment System for Enhancing Location Privacy of Electric Vehicles," IEEE Transactions on Vehicular Technology, vol. 63, no. 1, pp. 3-18, July. 2014.

〈저자소개〉

제이납 리자이파 (Zeinab Rezeifar) 학생회원
2008년: Shahid Bahopnar University of Kerman, Kerman, Iran 학사
2012년: Isfahan University of Technology, Isfahan, Iran 석사
2014년 3월~현재: 한양대학교 컴퓨터공학과 박사과정
〈관심분야〉 네트워크 보안, VANET, NDN, Network security,

오 희 국 (Heekuck Oh) 종신회원
1983년: 한양대학교 전자공학과 학사
1989년: 아이오와주립대학 전자계산학과 석사
1992년: 아이오와주립대학 전자계산학과 박사
1993~1994년: 한국전자통신연구원 선임연구원
1995년 3월~현재: 한양대학교 컴퓨터공학과 교수
〈관심분야〉 암호 응용, 악성코드 분석, 역공학