LOCATION PRIVACY ATTACKS AND DEFENSES IN CLOUD-ENABLED INTERNET OF VEHICLES

JIAWEN KANG, RONG YU, XUMIN HUANG, MAGNUS JONSSON, HANNA BOGUCKA, STEIN GJESSING, AND YAN ZHANG

ABSTRACT

As one of the promising branches of the Internet of Things, the cloud-enabled Internet of Vehicles (CE-IoV) is envisioned to serve as an essential data sensing, exchanging, and processing platform with powerful computing and storage capabilities for future intelligent transportation systems. The CE-IoV shows great promise for various emerging applications. In order to ensure uninterrupted and high-quality services, a vehicle should move with its own VM via live VM migration to obtain real-time location-based services. However, the live VM migration may lead to unprecedented location privacy challenges. In this article, we study location privacy issues and defenses in CE-IoV. We first present two kinds of unexplored VM mapping attacks, and thus design a VM identifier replacement scheme and a pseudonym-changing synchronization scheme to protect location privacy. We carry out simulations to evaluate the performance of the proposed schemes. Numerical results show that the proposed schemes are effective and efficient with high quality of privacy.

INTRODUCTION

With the rapid development of wireless communication technologies, the Internet of Vehicles (IoV) has been extended to include information interaction among vehicles, humans, and roadside infrastructures. Because of the requirements of small and low-cost hardware systems, a single vehicle normally has limited data processing capability. It is increasingly difficult for a single vehicle to efficiently support many emerging applications with complex computation and increasing storage demands. For example, in the scenario of autonomous driving, an autonomous vehicle may generate real-time navigation data at gigabits per second. It is necessary but challenging for vehicles to quickly process the massive collected surrounding information for path planning. To tackle this challenge, the IoV is evolving into a cloud-enabled IoV (CE-IoV) [1]. The CE-IoV combines the advantages of the IoV and cloud computing to dynamically integrate resources, and thus improve user experience.

In CE-IoV, vehicles obtain various location-based services (LBS) from third-party service providers (e.g., the gas stations within 1 km of the current location) [2]. Vehicles increasingly rely on different useful LBS, which are greatly improving the driving experience. In order to provide uninterrupted high-quality services and reduce large-scale data transmissions, the cloud manager first customizes virtual machines (VMs) for vehicles to support LBS according to the vehicles’ demands [3, 4]. Then the running VMs of the vehicles migrate from one cloud site to another according to the real-time locations of the vehicles. The vehicles send their service requests containing real-time locations and VM identities to third-party service providers to obtain ongoing LBS. This process is executed by live VM migration (LVM) technologies [5]. The routes of the LVMs are mapped to the corresponding mobility trajectories of the vehicles.

However, security and privacy issues cannot be neglected when vehicles obtain LBS from third-party service providers [2]. The third-party service providers are responsible for protecting the users’ privacy, and databases of the service providers are generally not public. But sensitive location information may still be misused or leaked by compromised or malicious providers, resulting in sensitive data leakage [4, 6]. In LBS, a series of service requests can be linked together through VM identities to infer the trajectories of the vehicles.

Moreover, for safe driving, vehicles are required to periodically broadcast their current locations, speeds, and accelerations in authenticated “safety messages” to surrounding neighbors using changing pseudonyms. These safety messages increase the awareness of vehicles about their neighbors’ whereabouts and warn drivers of dangerous situations. The location accuracy of safety messages is prominent for autonomous vehicles, which often travel at high speed and get close to each other [1]. In LBS applications of autonomous vehicles, higher location accuracy is meaningful to improve the quality of the LBS applications. The same location accuracy requirement is emphasized in CE-IoV. Nowadays, the accuracy of vehicle position is within...
Several meters, which will gradually be improved in the near future [7].

However, there are potential threats to location privacy of vehicles when the vehicles obtain high-quality LBS from third-party service providers [4, 6]. An adversary easily gets location information and pseudonyms of vehicles by eavesdropping safety messages. If the adversary also obtains sensitive data leaked by third-party service providers (e.g., VM identities of vehicles and location information), the adversary may exploit a mapping relationship between pseudonyms of safety messages and VM identities by matching the same location information. Finally, the adversary may infer the whole trajectory of the target vehicles by the mapping relationship, which results in location privacy leakage [8].

For traditional IoV, there are three categories of schemes for location privacy preservation:
1. Dummy generation-based schemes produce fake paths to confuse adversaries [2].
2. Obfuscation-based schemes use a group identity to replace vehicles’ real identities, such as group signature [9].
3. Anonymity-based schemes replace vehicles’ real identities by pseudonyms (e.g., silent period and Mix-zone).

On one hand, traditional location privacy issues have been researched without the existence of live VM migration, not taking potential misbehaviors of LBS into consideration. On the other hand, the aforementioned schemes may not work as well as expected in CE-IoV. The computation overhead of dynamic dummy generation algorithms cannot be ignored in CE-IoV. Group signature or pseudonym-changing schemes are useless as long as the VM identity of the target vehicle is located. Traditional location privacy preservation schemes are not sufficient to guarantee anonymity in CE-IoV.

In this article, we first describe the unexplored VM mapping attacks in CE-IoV, and propose a VM identifier replacement scheme to protect VM location privacy using random VM identifiers. We exploit a metric, quality of privacy (QoP), to quantify the level of location privacy (i.e., the linkability between location information and a vehicle). To further enhance the QoP, a pseudonym-changing synchronization scheme is proposed for privacy preservation.

The rest of the article is organized as follows. First, we describe the CE-IoV and the adversary model. Then two kinds of VM mapping attacks and defenses are described. Next, performance evaluation is provided. We then conclude the work.

**Cloud-Enabled Internet of Vehicles and our Adversary Model**

**CE-IoV and Live VM Migration**

CE-IoV exploits powerful computation and storage capabilities in the cloud environment with entities including vehicles, LBS providers, roadside units, and server clusters. These entities are described as follows [3].

**Central Cloud:** A central cloud is established among a group of dedicated servers on the Internet. There is a trusted registration authority in the central cloud, which issues and manages certificates for all entities. The registration authority could be a government transport department or an international trusted organization. Each entity applies its own certificate from the registration authority in order to confirm its qualifications.

**Local Cloud:** A local cloud consists of a set of adjacent roadside units. In a local cloud, there are some local cloud servers attached to the roadside units and a cloud manager. The cloud manager of a local cloud manages the local computing and storage resources, which can be rented by LBS providers to serve the vehicles. A vehicle accesses a local cloud by vehicle-to-infrastructure communications during driving.

**LBS Provider:** LBS providers offer various LBS utilizing computation resources rented from local clouds when vehicles request LBS (e.g., navigation service). To ensure services’ continuity and reduce system cost, it is necessary for vehicles to use LVM to obtain high-quality LBS during driving.

Figure 1 shows an example where a vehicle utilizes LBS for path planning in CE-IoV. A vehicle sends service requests to a cloud manager by vehicle-to-infrastructure communication. The cloud manager customizes a specific VM for the vehicle to support cloud services according to its demands. The vehicle uploads real-time location information and VM identity information via its corresponding VM to the LBS providers for service execution. The corresponding VM deals with all the data and assists the vehicle in making real-time decisions of path planning.

Compared to traditional security authentication schemes, LVM can avoid redundant authentication handshake protocols between vehicles and local clouds in CE-IoV [10]. Therefore, LVM not only reduces system load and overhead, but also improves efficiency, especially in the case of heavy traffic. Generally speaking, there are several steps during an LVM process as follows [5]:

- **Setup stage.** A TCP connection between the source and migration destination is set up according to the state information of a specific vehicle (e.g., current location, direction, and VM migration destination).
As shown in Fig. 1, a vehicle connects to the nearest roadside unit and then accesses the local cloud, which provides access to the vehicle’s VM. The VM communicates with the LBS provider and returns the service data to the vehicle. When a vehicle is driving on the road without service interruption, the trajectory of the LVM among local clouds is mapped to part of the vehicle’s actual trajectory [8]. When the adversary analyzes and establishes the mapping relationship between the vehicle’s true identity and the corresponding VM, the problem of location privacy leakage occurs.

For safe driving, vehicles periodically broadcast safety messages \{\textit{Pseudonym, Location, Velocity, Content, Time}\} to surrounding neighbors. Each vehicle carries a set of pseudonyms and uses random pseudonyms for safety message broadcasts. Then the vehicle periodically changes pseudonyms without reuse for privacy preservation. At the same time, a vehicle obtains LBS via its own unique VM identity. However, in the cloud environment, the LBS providers may not satisfy the privacy preservation requirements of vehicles. Without doing any privacy preservation measurement of the cloud platforms, LVM is at risk of privacy exposure.

We consider that the adversary in this article is a typical global external adversary described in [9], which can eavesdrop and collect global safety messages in the network. The adversary distributes a group of monitor devices in the areas of observation points to collect traffic-related information. But the adversary cannot monitor the traffic of the entire network. We consider that the adversary uses radio-based eavesdropping, which only involves moderate system cost. The adversary can observe the ongoing LVM process from compromised LBS providers, and also eavesdrops the safety message broadcasts of vehicles. Both data leakage of third-party services and safety messages is mapped to part of the vehicle’s actual trajectory. The adversary attempts to make use of such information to establish the mapping relationship between pseudonyms and VM identities by matching the same specific location information, which raises serious concerns about location privacy. In this case, the adversary is helped by the precise safety messages to detect, classify, and locate a target vehicle, even though there are many vehicles around the same time in the same area. For example, at an intersection, the adversary can judge whether its target vehicle leaves from here by observing the same location change of safety messages and LVM. Two unexplored attacks called VM mapping attacks are proposed in the next section.

**Virtual Machine Mapping Attacks and Defense Schemes**

In this section, we introduce two typical VM mapping attacks, observation mapping attack and linkage mapping attack, followed by corresponding defense schemes.

**Observation Mapping Attack and Defense**

Observation Mapping Attack: Generally, an adversary stays in one region or moves through a pre-defined movement strategy to observe a
target vehicle. Figure 2 shows a vehicle uploading its real-time locations to an LBS provider for various services. Meanwhile, the vehicle broadcasts safety messages including locations and pseudonyms to neighbors for safe driving. Then the adversary not only gets the VM’s identity and real-time locations from an LBS provider, but also receives the vehicle’s pseudonyms and real-time locations by eavesdropping the safety messages.

When an adversary wants to track a target vehicle using a specific pseudonym (e.g., V_b in Fig. 2), the adversary observes the target vehicle more than one sample period in order to establish the mapping relationship between VM identity (VM_1) and the vehicle’s pseudonyms. On one hand, nowadays, the accuracy of vehicular position is within several meters. There is no doubt that this accuracy will gradually be improved in the future [7]. On the other hand, vehicles often travel at speeds of 40 to 65 miles per hour on the highway or in an urban area [12]. Generally, the probability of vehicles staying close to the same area is quite low after long-term observation (e.g., half an hour). So we consider that the real-time location information (e.g., half an hour). So we consider that the real-time location information Location_1 is unique and accurate, the mapping relationship (VM_1 corresponding to V_a) can be established by Location_1. Similarly, VM_1 corresponds to V_b at Location_2, and VM_1 corresponds to V_c at Location_3. As the VM identity VM_1 is unchanged during driving, the adversary can easily re-identify the target vehicle by monitoring VM_1’s locations. Although the target vehicle updates its pseudonym from V_a to V_b, and then from V_b to V_c between Location_1 to Location_3, the adversary can confirm the target vehicle by the real-time locations of VM_1. This attack is called observation mapping attack. The adversary obtains the pseudonym history of the target vehicle via uninterruptedly observing the real-time locations of the VM of the target vehicle. Then the adversary establishes the mapping relationship between pseudonyms and the target vehicle’s VM for restoring the whole trajectory. For example, VM_1 corresponds to {V_a, V_b, V_c}.

Defending against Observation Mapping Attack: An observation mapping attack results from the mapping relationship between pseudonyms of a target vehicle and its unique VM identity. Generally speaking, one straightforward solution is to replace the VM identity by random identifiers and periodically change the identifiers, which makes the mapping relationship fail. In this article, we propose a VM identifiers replacement scheme (VIRS). In this scheme, every VM obtains a certain number of random identifiers from the local cloud. The VMs periodically change their identifiers to apply for services.

We first introduce the framework of VIRS. Figure 3 shows that a registration authority is in charge of authentication between local clouds and vehicles. There are four parts of the registration authority: register database, VM identifiers database, mapping database, and blacklist pool of vehicles. More details are given below:

• The register database stores all the register information of vehicles including license plate numbers, owners’ names, and identities. The register database generates an information mapping table from the vehicles to the owners.
• The VM identifiers database is a database of all identifiers used to make VMs anonymous. The central cloud randomly allocates a number of VM identifiers to the local cloud. The local cloud stores these VM identifiers in a VM identifier pool, and the VM manager in this local cloud manages these VM identifiers.
• The mapping database is used to record the mapping relationships between vehicles and their corresponding VM identifiers.
• All the blacklists of vehicles in CE-IoV are updated and gathered to the blacklist pool in the central cloud.

Figure 3 shows the key steps of the VM identifiers replacement scheme.

Step 1: A vehicle sends its personal identity information and a service request after encryption to the local cloud via an adjacent roadside unit. The vehicle will be authenticated after the local cloud transmits the identity information to the registration authority.

Step 2: In the local cloud, a VM manager randomly distributes n VM identifiers to an authenticated vehicle, which are chosen from the local VM identifier pool. The VM manager records and generates a mapping list between the vehicle and its obtained VM identifiers, and then uploads the mapping list to the mapping database in the central cloud.

Step 3: The vehicle uses different VM identifiers to request LBS for privacy preservation. When a VM identifier has expired, a new one is used. The expired identifiers will be recycled after the VM manager has recaptured these expired identifiers back to the VM identifier database of the central cloud. These VM identifiers will be redistributed to other local clouds in the next round.

Step 4: After having used n identifiers, the vehicle should send its new request to the local cloud for obtaining new VM identifiers.
Figure 4. Linkage mapping attack.

If a vehicle is found to be malicious or compromised, its true identity will be exposed with the help of the mapping database and register database in the central cloud. The identity-related information of the vehicle will be added to the blacklist and sent to the blacklist pool in the central cloud. Some compromised third-party entities can be found out by the registration authority, which is in charge of monitoring the behaviors of third-party entities. Then the central cloud generates a revocation list containing two kinds of entities: malicious or compromised vehicles and third-party entities. The central cloud sends the updated revocation list to all local clouds for broadcasting this list to all vehicles. The communications among the vehicles include safety message broadcasts and normal message communication by vehicle-to-vehicle technology (e.g., dedicated short-range communications). When a vehicle communicates with another vehicle or a third-party entity, they first send handshake protocols to each other for identity verification. The handshake protocols include identity-related information and corresponding signatures of the vehicles or third-party entities. According to the identity-related information in the handshake protocols, the vehicle checks whether another entity or vehicle is trusted within a time period. Therefore, the legitimate vehicles refuse to communicate with the malicious vehicles or third-party entities included in the newest revocation list, which improves secure communication and decreases the probability of privacy leakage [9, 13].

**LINKAGE MAPPING ATTACK AND DEFENSE**

**Linkage Mapping Attack:** To further improve the degree of privacy protection of the VIRS, it may not be enough to only use the VIRS. This is because the adversary may re-identify the target vehicle through further discovering the linkage of background information. In a road network, vehicles’ movements are constrained by many spatial and temporal factors including physical roads, directions, speed limits, and traffic conditions. Vehicles use pseudonyms for safety message broadcasts and the VIRS for privacy preservation during the LBS process. However, a new potential threat arises when the processes of VM identity replacement and pseudonym changing are asynchronous. Suppose an adversary knows a target vehicle’s pseudonym $V_e$ through the linkage of background information. The adversary tries to link the $V_e$ with one specific VM identifier for re-identifying the target vehicle, which is defined as a linkage mapping attack.

Figure 4 shows that a vehicle replaces its VM identifiers for LBS requests every time period $T_1$, and changes its pseudonyms for safety message broadcast every time period $T_2$ (here, we consider $T_1 > T_2$). Starting from a certain moment $T_0$, the vehicle starts to use $VM_1$ as a new VM identifier, and then changes $VM_1$ to $VM_2$ at $T_1$. The vehicle keeps the VM identifier $VM_2$ until $T_2$. Meanwhile, the vehicle changes its pseudonyms for safety message broadcasts from $V_a$ to $V_d$ step by step every time period $t_2$ between $t_0$ and $t_1$. From $t_0$ to $t_1$, the vehicle uses $VM_1$ to request LBS. During the same time interval, the vehicle broadcasts safety messages using pseudonyms from $V_a$ to $V_d$. An adversary makes use of the mapping relationship between the VM’s identifiers and the vehicle’s pseudonyms, that is, $VM_1$ corresponding to $\{V_a, V_b, V_c, V_d\}$, to track the target vehicle. Although the vehicle’s pseudonyms are changed from $t_0$ to $t_1$, its VM identifier is still $VM_1$. Consequently, the adversary can re-identify the target vehicle via $VM_1$. Similarly, the vehicle replaces $VM_1$ by $VM_2$ at time $t_1$, but the adversary observes that the vehicle’s pseudonym is not changed at $t_1$ (still $V_d$). Then the adversary establishes the mapping relationship (e.g., $V_g$ corresponding to $\{VM_1, VM_2\}$) to re-identify the target vehicle. Finally, the adversary links $\{VM_1, VM_2\}$ to $\{V_a, V_b, V_c, V_d, V_e, V_f, V_g\}$, and thus reconstructs the trajectory of the target vehicle in the geographic space. This brings a low privacy protection level, resulting in serious location privacy leakage.

**Defending against Linkage Mapping Attack:** A linkage mapping attack is mainly due to asynchronism between pseudonym changing and VM identity replacement. The adversary makes use of the mapping relationship between VM identifiers and pseudonyms to reconstruct sensitive location information of the target vehicle, even the whole trajectory history. A pseudonym changing synchronization scheme (PCSS) is proposed to defend against this attack. In this scheme, the process of pseudonym changing and VM identity replacement is synchronized to defend against linkage mapping attacks, which enhances the privacy protection level during driving. There are several key steps in the PCSS as follows.

**Step 1:** A vehicle checks the time with the VM manager of the local cloud to achieve time synchronization.

**Step 2:** The vehicle sends a VM identifier change request to the VM manager. After the agreement of the VM manager, the vehicle chooses a new VM identifier from its legitimate VM identifiers and uploads it to the VM manager for verification. The VM manager checks the vehicle’s information, and transmits the vehicle’s identity and its VM identifier to the central cloud. The registration authority in the central cloud verifies whether that VM identifier belongs to this vehicle. If yes, the registration authority will record this replacement event and establish the mapping relationship between the VM identifier and the vehicle according to the order of time. The mapping relationship will help to facilitate accountability for credentials when dispute or revocation occurs.
Step 3: The VM manager responds to the request from the vehicle, and prepares for the changing of the vehicle’s VM configuration parameters.

Step 4: The vehicle sets a suitable time window $T^*$ to change the VM identifier. The vehicle sends the $T^*$ to the VM manager for notifying the VM manager to prepare for the replacement.

Step 5: Before $T^*$, the vehicle periodically communicates with the VM manager and checks the time until both of them are well prepared.

Step 6: At $T^*$, both the vehicle and the VM manager synchronously perform pseudonym changing and VM identifier replacement, respectively. After that, the vehicle can broadcast safety messages with an updated pseudonym, and request LBS via a new VM identifier.

**Quality of Privacy and Numerical Results**

Generally speaking, the location privacy level is quantified as the uncertainty of location information related to a specific vehicle, which is defined as QoP. Here, the QoP is calculated by $H = -\sum p_i \log_2 p_i$, where $p_i$ denotes the probability that a vehicle under observation is the target vehicle. Higher $H$ represents bigger QoP and consequently a higher location privacy level [8].

We carry out simulations to evaluate the performance of our proposed schemes by the QoP. We use synthetic vehicle traces and road maps to simulate different sizes of observation regions [12]. More specifically, the coverage area of each local cloud is set to 4 km$^2$. A small observation region with combined local clouds is 20 km$^2$ and a large observation region is 40 km$^2$. The changing period of pseudonyms about safety message broadcasts is 1 min. An adversary observes these combined regions of local clouds, in which 100 vehicles randomly move in the road map and periodically change pseudonyms of safety message broadcasts. Every vehicle is allocated a running VM while driving. The radio coverage radius of roadside units and vehicles is set to be 500 m, which is a typical range of the IEEE 802.11p WAVE protocol. There are three scenarios with different location privacy preservation strength. First, the vehicles move in the observation regions without changing VM identifiers, which is called VM identifiers without replacement (VIWR). Second, the vehicles carry a certain number of VM identifiers and perform asynchronous changing between pseudonyms and VM identifiers via our proposed VIRS. Finally, the vehicles perform synchronous changing between pseudonyms and VM identifiers via our PCSS.

Figure 5 shows the performance comparison of different scenarios. The horizontal axis is the number of VM identifiers carried by a vehicle when accessing the observation regions. The vertical axis represents the average value of privacy entropy (i.e., QoP) among the observed vehicles. Figure 5 shows that our proposed schemes with VM identifier replacement perform better than that of the VIWR. This is because the vehicles without VM identifier replacement are easier to track. In VIWR, we consider that an adversary wants to track a target vehicle. Before discovering the target vehicle, the adversary randomly chooses one vehicle as its target to observe the vehicle’s VM identifier and safety messages. As there are 100 vehicles in the observation region, the probability of success (that the observed vehicle is the target vehicle) is 0.01 in this scenario. The QoP of the VIWR is the lowest in both large and small observation regions, which is a baseline for reference. When the vehicles access a large region with 10 VM identifiers, the QoP of the PCSS is about 10 percent larger than that of the VIRS. This is because even though the vehicles change VM identifiers in the VIRS to defend against the adversary, the adversary may perform a linkage mapping attack to make some of the VM identifiers invalid. Comparing the QoP in different regions, the larger region brings higher QoP resulting from lower $p_i$.

To compare the overhead of our PCSS with the existing dummy generation algorithm proposed in [2], we consider that a certain number of vehicles randomly drive in a large observation region using our PCSS scheme and an Enhanced Dummy Generation Algorithm (EDGA) scheme, respectively. The EDGA scheme is extended and developed according to the dummy generation algorithm scheme, which not only generates $k$ fake paths of vehicles, but also generates $k$ corresponding fake paths of VMs for privacy preservation. We assume that the spots of fake paths in the EDGA scheme are the locations of changing pseudonyms in the PCSS. We use privacy entropy to compare these two schemes. As the EDGA scheme has no VM identifiers, for simplicity, we transform the privacy entropy achieved by the EDGA scheme into the equivalent privacy entropy obtained via VM identifiers. Figure 6 shows the total number of used VM identifiers (i.e., overhead) in different schemes with the same privacy entropy. When the number of vehicles increases, the total number of used VM identifiers increases. That is, the overheads of both schemes increase with the number of vehicles. More fake paths generated by the EDGA bring higher overhead. To achieve the same privacy...
entropy, the overhead of the EDGA scheme ($k = 2$) is 80 percent more than that of the PCSS when the number of vehicles is 300. In summary, according to Figs. 5 and 6, our schemes for privacy preservation are effective and efficient with high QoP for safe driving.

**CONCLUSION AND OPEN ISSUES**

In this article, we have presented two virtual machine mapping attacks and defenses for LVM in CE-IoV. We first introduce the CE-IoV model and the LVM process, and then describe location privacy followed by two typical virtual machine mapping attacks. We propose two defense schemes and then evaluate the performance of our schemes. Results showed that our schemes for privacy preservation are effective and efficient with high QoP. The results are important for CE-IoV in general, but especially for secure driving applications.

There are several interesting problems that are worthy of further study, such as secure frameworks of live VM migration for LBV, and secure data search and storage [14, 15]. In particular, we will focus on two new challenges for privacy preservation:

1. The QoP in pseudonym-based schemes depends on the uncertainty (i.e., privacy entropy) in mapping pseudonyms to real identities from the perspective of adversaries. Simply replacing the VM’s real identifiers with pseudonyms may be insufficient to guarantee good anonymity. It is an open issue to improve the QoP of pseudonym-based schemes, or replace pseudonym-based schemes by other schemes (e.g., group-signature-based schemes).

2. In a dynamic topology, the communication protocols in a privacy preservation scheme between vehicles and local clouds should be safe and efficient to reduce system cost.

**ACKNOWLEDGMENT**

The work is supported in part by programs of NSFC under Grant nos. 61422201, 61370159, and U1201253, U1301255, the Science and Technology Program of Guangdong Province under Grant no. 2015B010129001, Special-Support Project of Guangdong Province under grant no. 2014TQ01X100, High Education Excellent Young Teacher Program of Guangdong Province under grant no. YQ2013057, Science and Technology Program of Guangzhou under grant no. 2014J2200097 (Zhujiang New Star Program), and is partially supported by the projects 240079/F20 funded by the Research Council of Norway, and the Polish Ministry of Science and Higher Education within the status activity task “Cognitive radio systems” in 2016.

**REFERENCES**


**BIOGRAPHIES**

JIAWEN KANG ([jiawen.kang.cn@ieee.org]) received his M.S. degree from Guangdong University of Technology, China, in 2015. He is now pursuing his Ph.D. degree at the same university. His research interests mainly focus on resource management, security, and privacy protection in wireless communications and networking. He is the author or co-author of 13 papers published in journals, magazines, and proceedings of international conferences.

RONG YU ([yurong@ieee.org]) received his Ph.D. degree from Tsinghua University, China, in 2007. After that, he worked in the School of Electronic and Information Engineering of South China University of Technology (SCUT). In 2010, he joined the Institute of Intelligent Information Processing at Guangdong University of Technology, where he is now a full professor. His research interests mainly focus on wireless communications and networking, includ-
ing cognitive radio, wireless sensor networks, and home networking. He is the co-inventor of over 10 patents and author or co-author of over 100 international journal and conference papers. He is currently serving as the deputy secretary general of the Internet of Things (IoT) Industry Alliance, Guangdong, China, and the deputy head of the IoT Engineering Center, Guangdong, China. He is a member of the Home Networking Standard Committee of China, where he leads the standardization work on three standards.

XUMIN HUANG (huangxu_min@163.com) is now a Master’s student of networked control systems at Guangdong University of Technology. His research interests mainly focus on network performance analysis, simulation, and enhancement in wireless communications and networking.

MAGNUS JONSSON [SM] (Magnus.Jonsson@hh.se) received his B.S. and M.S. degrees from Halmstad University, Sweden, in 1993 and 1994, respectively, and his Licentiate of Technology and Ph.D. degrees from Chalmers University of Technology, Gothenburg, Sweden, in 1997 and 1999, respectively, all in computer engineering. Since 2003, he has been a full professor of real-time computer systems at Halmstad University, where he is also the vice dean and director of research of the School of Information Technology (ITE). From 1998 to March 2003, he was an associate professor of data communication at Halmstad University (between 1998 and 2000). He has published close to 120 scientific papers and book chapters, most of them in the areas of vehicular communication, real-time communication, industrial communication, wireless networking, real-time and embedded computer systems, optical networking, and optical interconnection architectures.

HANNA BOGUCKA [SM] (hbogucka@et.put.poznan.pl) received her Ph.D. degree and Doctor Habilitus degree in telecommunications from Poznan University of Technology (PUT), Poland, in 1995 and 2006, respectively. Currently, she is a full professor and deputy dean for research in the Faculty of Electronics and Telecommunications at PUT. She is involved in research in the area of wireless communications: cognitive radio and energy-efficient wireless systems and networks. She has been involved in projects funded by the Polish National Science Centre, and the Ministry of Science and Higher Education, and has consulted for the Polish telecommunications operator. She has been involved in multiple European 5th and 7th Framework Programme and Horizon 2020 projects dealing with novel flexible and cognitive radio technologies. She is the author of over 150 papers, published in major IEEE journals and magazines, European journals, and the proceedings of international conferences. She is also the author of one book and a number of book chapters focusing on green communications and cognitive radio. She was the IEEE Communications Society Director of the EAME Region (Europe, Africa, Middle East) for 2014–2015 and the IEEE Radio Communication Committee Chair for 2015–2016.

STEIN GIESSING [M] (steing@ifi.uio.no) received his Ph.D. degree in 1985, and is currently a professor of computer science in the Department of Informatics, University of Oslo, and an adjunct researcher at Simula Research Laboratory. His original work was in the field of object-oriented concurrent programming. He has worked with computer interconnects (Scalable Coherent Interface, IEEE Std. 1596) and LAN/MANs (Resilient Packet Ring, IEEE Std. 802.17). His main research interests are currently network and transport protocols, network resilience, cognitive radio networks, vehicular networks, and the smart grid.

YAN ZHANG [SM] (yanzhang@ieee.org) is currently head of the Department of Networks at Simula Research Laboratory, Norway, and an associate professor (part-time) at the Department of Informatics, University of Oslo, Norway. He received a Ph.D. degree from the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore. He is an Associate Editor or on the Editorial Board of a number of well-established scientific international journals, such as Wiley’s Wireless Communications and Mobile Computing. He has also served as a Guest Editor for IEEE Transactions on Industrial Informatics, IEEE Communications Magazine, IEEE Wireless Communications, and IEEE Transactions on Dependable and Secure Computing. He has served in Chair positions for a number of conferences, including IEEE PIMRC 2016, IEEE CCNC 2016, WICON 2016, IEEE SmartGridComm 2015, and IEEE CloudCom 2015. He has also served as a TPC member for numerous international conference including IEEE INFOCOM, IEEE ICC, IEEE GLOBECOM, and IEEE WCNC. His current research interest include wireless networks and reliable and secure cyber-physical systems (e.g., healthcare, transport, smart grid). He has received seven Best Paper Awards. He is a Senior Member of IEEE ComSoc and the IEEE Vehicular Technology Society.

The authors proposed two defense schemes and then evaluated the performance of our schemes. Results showed that our schemes for privacy preservation are effective and efficient with high QoP. The results are important for CE-IoV in general, but especially for secure driving applications.