Security, Privacy, and Fairness in Fog-Based Vehicular Crowdsensing

Jianbing Ni, Aiqing Zhang, Xiaodong Lin, and Xuemin (Sherman) Shen

The authors examine the architecture, applications, and especially security, privacy, and fairness of fog-based vehicular crowdsensing. They introduce the overall infrastructure and some promising applications, including parking navigation, road surface monitoring, and traffic collision reconstruction, then study the security, privacy, and fairness requirements, and describe the possible solutions to achieve security assurance, privacy preservation, and incentive fairness.

ABSTRACT

Fog-based vehicular crowdsensing is an emerging paradigm where vehicles use onboard sensors to collect and share data with the aim of measuring phenomena of common interest. Unlike traditional mobile crowdsensing, fog nodes are introduced specifically to meet the requirements for location-specific applications and location-aware data management in vehicular ad hoc networks. In this article, we examine the architecture, applications, and especially security, privacy, and fairness of fog-based vehicular crowdsensing. Specifically, we first introduce the overall infrastructure and some promising applications, including parking navigation, road surface monitoring, and traffic collision reconstruction. We then study the security, privacy, and fairness requirements in fog-based vehicular crowdsensing, and describe the possible solutions to achieve security assurance, privacy preservation, and incentive fairness. By defining interesting future directions, this article is expected to draw more attention into this emerging area.

INTRODUCTION

The integration of sensors and embedded computing devices triggers the emergence of mobile crowdsensing services [1], which allows individuals to cooperatively collect and share data and extract information to measure and map phenomena of common interest using sensing and communication technologies. With the increasing popularity of mobile devices, mobile crowdsensing becomes a broad range of sensing paradigms nowadays. For example, an iPhone 6S can sense the environment with a rich set of sensors, including a camera, GPS, a proximity sensor, and a barometric sensor, to generate and share the sensing reports with interested parties [2].

Similar to mobile phones, modern vehicles are also equipped with onboard sensors and wireless communication devices [3], such as cameras, GPS, tachographs, lateral acceleration sensors, and onboard units (OBUs), providing fundamental capability and feasibility of vehicular crowdsensing. By using OBUs and sensing devices, vehicles can not only periodically report the driving information (e.g., location, real-time speed, and driving video) but also incidentally provide traffic conditions, road conditions, and weather conditions for transportation planning, road system design, traffic signal control, and so on [4]. The approach of raw data acquisition through vehicular crowdsensing significantly reduces the financial and time cost for data customers. With the development of electric devices in vehicles, the sensing data become increasingly fine-grained and complex, so the data from vehicles are extended to support more applications, such as vehicle fault diagnostic, vehicle noise pollution detection, and air quality forecast. Meanwhile, fine-grained data collection increases the burden on data transmission and centralized data management. The cloud server has to maintain and process data for supporting vehicular crowdsensing services. Nevertheless, local relevance is one of the important features of vehicle-generated data, which means that the sensing data have their own spatial scope and explicit lifetime of utility. For example, traffic congestion information may only be valid for 30 minutes and of interest to the vehicles that are approaching a traffic jam area. Vehicle-generated contents are also local interests, indicating that the traffic and road condition information of a specific region are only of interest to the vehicles in or near that region. Therefore, centralized data management is not recommended, and the sensing data should be classified according to the spatial-temporal information.

Fog computing is a particularly attractive paradigm [5] that utilizes network edge devices to carry out a substantial amount of storage, communication, and computing close to the mobile devices, so it is not necessary to send all data all the way to the cloud. With temporary data storage, computing, and processing, the constraints of the information interactions between the cyber world and physical world, in terms of latency, load balancing, and fault tolerance, can be released. These appealing advantages trigger the emergence of fog-based vehicular crowdsensing (FVCS). On behalf of local servers, vehicular fog nodes can temporarily store and analyze the sensing data uploaded by vehicles to provide local services (e.g., real-time navigation, parking space reservation, and restaurant recommendation). They can process the data locally and pass the results to interested vehicles quickly, thereby saving unnecessary wireless bandwidth for transmitting the raw data to a remote cloud server and also supporting location-aware data management. Therefore, FVCS not only inherits the advantages of mobile crowdsensing [1], but also integrates fog computing to have unique characteristics, including location awareness, geo-distribution, and communication efficiency. However, security and privacy

Digital Object Identifier:
10.1109/MCOM.2017.1600679

Jianbing Ni is with the University of Waterloo; Aiqing Zhang is with Anhui Normal University and the University of Ontario Institute of Technology; Xiaodong Lin is with the University of Ontario Institute of Technology; Xuemin (Sherman) Shen is with the University of Waterloo.

in such infrastructure are very challenging. In fact, neither a cloud nor fog service provider is fully trusted, and vehicles are unlikely to share their collected data with strangers. Without a trusted mediator, privacy is easily violated, and vehicles will probably be uncooperative in uploading their data to fog nodes, although incentive mechanisms are built to encourage mobile users and compensate their cost on data collection. Therefore, sustainable crowdsensing supporting incentive, security, and privacy preservation is of significant importance in FVCS.

As indicated above, despite the tremendous benefits brought by FVCS, the infrastructure is still confronted with many security and privacy challenges, including sensitive information leakage, impersonation attacks, and Sybil attacks. Recently, extensive research efforts [6–8] have been made to cope with these challenges in mobile crowdsensing. However, the overall infrastructure and security and privacy issues in FVCS have not been systematically studied. Clearly, to study security and privacy requirements and their relationships to the unique characteristics of FVCS is very critical prior to the design of any specific schemes. In this article, we first define the infrastructure of FVCS and discuss its promising applications. We then explore the security, privacy, and fairness requirements, and the research challenges in FVCS. In addition, we describe three state-of-the-art solutions to address the security, privacy, and fairness challenges, respectively. Last, we present some interesting and promising future research directions.

Architecture of Fog-Based Vehicular Crowdsensing

A vehicular ad hoc network (VANET) is formed as a self-organized network to facilitate inter-vehicle communications, vehicle-to-roadside communications, and Internet access with relay by roadside units (RSUs). Vehicular fogs are upgraded RSUs that stretch to have computational capabilities and storage spaces for offering a certain of computational and storage services to vehicles. FGVS is a virtual environment, composing of a cloud, vehicular fogs, vehicles, and customers.

Cloud: The cloud has huge storage and computational capabilities for providing vehicular crowdsensing services to customers. It not only communicates with the customers for releasing crowdsensing tasks and delivering results, but also collect crowdsensing reports from vehicular fogs and assign benefits to vehicles.

Vehicular Fogs: The vehicular fog nodes are equipped with enhanced storage space, computational and communication devices and placed on the edge devices of the Internet, usually deployed along the road-side or at critical points, e.g., junctions and parking lots. They use short range communication devices to communicate with the driving-through vehicles in their coverage regions for collecting crowdsensing reports and deliver crowdsensing reports to the cloud through wired connections. Intuitively, RSUs in traditional VANETs can be enhanced by introducing computing and storage capability to them to act as fog nodes.

Vehicles: Each vehicle is installed with an unreplaceable and tamper-proof device, the OBU, which can communicate with nearby vehicles and vehicular fogs. The OBU enables some simple computations to be performed, collects the data from onboard sensing devices, and uploads data to the nearby fog nodes.

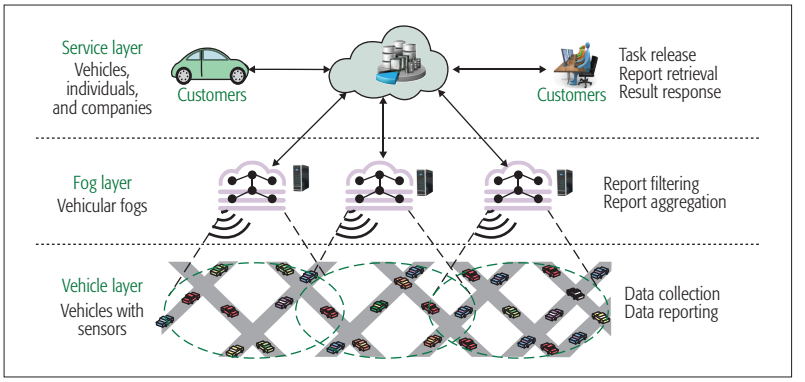

Figure 1. Architecture of fog-based vehicular crowdsensing.

Customers: Customers can be vehicles, individuals, and organizations. They have insufficient capabilities to perform the vehicular crowdsensing tasks by themselves, so they crowdsource the tasks to the cloud and give benefits to reward the vehicles who make contributions to their tasks.

As depicted in Fig. 1, the architecture of FVCS consists of three layers: the service layer, fog layer, and vehicle layer. In the vehicle layer, the vehicles driving on roads periodically and incidentally collect the traffic and road information using the onboard sensing devices and upload them to the local fog nodes. In the service layer, the customers outsource their tasks to the cloud, along with the benefits to reward the vehicles who contribute to their tasks. Then the cloud releases the tasks to the vehicular fog nodes located in the sensing areas. According to the tasks, the fog nodes find the right crowdsensing reports and return them to the cloud if the required data are on hand. Otherwise, the fog nodes have to allocate the tasks to the moving vehicles in the sensing area to acquire the necessary data. The cloud receives the crowdsensing reports from the fog nodes, and generates the results for the customers. Finally, the cloud assigns benefits to reward the vehicles who submit valuable data based on the comments of customers.

Applications

In this section, we briefly introduce some applications of FVCS, including parking navigation, road surface monitoring, and traffic collision reconstruction, as shown in Fig. 2.

Parking Navigation

Parking in a congested area (e.g., downtown and shopping malls), particularly in peak hours, is a conflicting and confusing problem for a large number of drivers. Circulating vehicles may cause extra traffic on roads and serious social problems (e.g., fuel waste, traffic congestions, air pollution, and vehicle accidents). Real-time parking information can assist drivers to find available parking spaces quickly. Nevertheless, it is pretty different to collect and publish the parking information, particularly for the roadside parking information. The video cameras on vehicles can record the driving scene, from which the cloud can acquire the information about vacant parking spaces on the streets and in parking

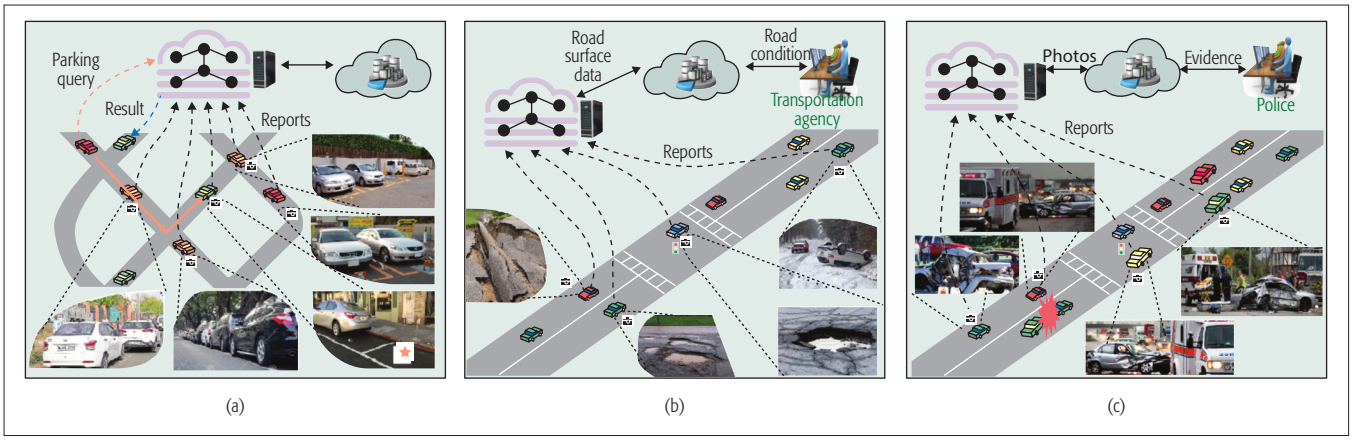

Figure 2. Applications of fog-based vehicular crowdsensing.

lots. Therefore, the moving vehicles can upload the driving videos or photos to the fog nodes, and a vehicle seeking a parking space can send a parking query to the cloud, including its destination, arrival time, and expected price. The cloud retrieves and analyzes the video and photos from the fog node covering the destination to find a vacant parking space for the querying vehicle.

Road Surface Monitoring

The detection of road surface abnormalities (e.g., potholes, bumps, ice, railway crossing) and their locations contribute to the improvement of road conditions and drivers' safety. Road quality assessment has been identified as an important issue related to the possibility of making drivers and passengers more comfortable and safe more efficiently. The presence of road damage or abnormalities also worsens the energy efficiency of vehicles driving through, since it determines an increase in fuel and consumption of vehicles' components, especially brakes and suspensions. The sensing devices on vehicles (e.g., GPS, accelerometer, and camera) offer the possibility of obtaining real-time information about road features. The vehicles can upload road conditions to fog nodes. Transportation agencies or municipalities can query the road surface abnormalities in the region of their jurisdiction to the cloud, and the cloud can automatically recognize the road problems for prioritizing road repair according to the data in fog nodes located in that region.

Traffic Collision Reconstruction

After an accident occurs, particularly one resulting in severe injuries or fatalities, the police usually investigate and reconstruct the accident with the intention to determine whether any criminal activity took place (e.g., speeding, alcohol use, drug use, or mechanical violations). For instance, if a truck driver falls asleep because of fatigue and causes a serious accident, this driver may be criminally charged with homicide if the resulting accident results in a fatality. Therefore, how to reconstruct the accident as the basis of evidence is significantly important for law enforcement. The videos on nearby vehicles can provide essential evidence for accident forensics. Nevertheless, these vehicles leave quickly, although they record the accident scene. In FVCS, the vehicles upload the sensing data to the nearby fog node, including the videos and photos. The police can query the evidence of an accident to the cloud, and the cloud can search the evidence on the fog node covering the accident position. In this way, the police are able to obtain the critical evidence to reconstruct the accident and identify the liability of each party involved.

Security, Privacy, and Fairness Challenges

Given the increasing interest in FVCS applications, the time is ripe to explore security and incentive challenges. Once the data is uploaded to the fog nodes, the vehicles lose control over their collected data. Neither a fog nor cloud service provider is fully trusted, and they are vulnerable to compromise. The corruption of crowdsensing reports may directly impact the results, and further mislead customers to make irrational decisions. Therefore, crowdsensing data presents critical security challenges, and data protection is significantly important for both vehicles and customers. Besides, to build successful FVCS applications, the cloud should recruit a large number of vehicles to participate in crowdsensing tasks. Nevertheless, performing tasks may incur monetary costs and network bandwidth usage, so vehicles may be reluctant to do it voluntarily. Therefore, how to provide sustainable and fair incentives to encourage vehicles to participate in vehicular crowdsensing services without sacrificing the security and privacy of vehicles is also critical in FVCS.

Security

FVCS entails serious security threats. First, onboard sensors collect data from the surrounding environment, which may contain a lot of sensitive information. Curious entities, including the fog service providers, cloud service providers, or vehicles, and external attackers, such as malicious hackers, are able to extract various types of personal information from crowdsensing reports (e.g., location, preferences, health status, and political affiliation). Furthermore, an attacker may infer secret information from the intersection of multiple crowdsensing reports. For example, the trajectory of a specific vehicle can be exposed from a plurality of successive reports. Therefore, the confidentiality of crowdsensing reports is the primary objective to achieve. Data encryption can be employed to protect sensitive information against curious

attackers. Nevertheless, customers are undermined when vehicles upload reports to fog nodes. Thus, data encryption triggers huge obstacles on data search and sharing. Proxy re-encryption with keyword search [9] is promising to allow the cloud to search for requested reports on fog nodes and share the matched data to customers on behalf of a proxy. However, after uploading the crowdsensing reports, the vehicles stay offline, indicating that it is difficult to find the vehicles to generate the proxy re-encryption keys when needed. Therefore, delegable key management in FVCS is significantly important and promising to focus on.

Second, authentication is another critical aspect related to the functionality of crowdsensing reports. If these reports are delivered by untrusted or malicious vehicles, the customers may be confused and make false decisions. Therefore, it is worthwhile to ensure that the sources of crowdsensing reports are fully trusted and behave honestly. Attacks on the crowdsensing reports can be divided into impersonation attacks and Sybil attacks [10]. In impersonation attacks, malicious attackers may pretend to be honest for reporting data, such that they can be rewarded benefits and insert forged reports to mislead customers. In Sybil attacks, malicious attackers may forge various identities to deliver different or identical reports to get more rewards or succeed in the statistical selection process on reports, respectively. To resist impersonation attacks and Sybil attacks, blacklist-based authentication should be built, and efficient detection methods on Sybil attackers are needed for the cloud. In addition, the lack of authentication on customers also brings troubles on task releasing. Specifically, the attackers may crowdsource invalid tasks to the cloud spitefully and obtain the crowdsensing results released by honest customers to enjoy free crowdsensing services. Therefore, it is necessary to guarantee that only honest customers and vehicles can participate in the activities of vehicular crowdsensing.

Privacy

The sensing data from the surrounding environment are necessarily people-centric and related to some aspects of the drivers or passengers and their social setting: where drivers and passengers are and where they are going; what places they frequently visit and what they are seeing; which trajectory they choose, and which activity they prefer to do in vehicles. For example, a driver Alice may want to report a traffic jam downtown to the nearby fog node, without the fog node knowing that Alice may be in congested downtown traffic at the time she reports the event. Since the fog node is location-aware, a vehicle is easy to locate based on the accessing fog node through which the vehicle makes a network connection. One solution is to use an anonymizing network to hide the vehicle's location while it is reporting data. However, anonymizing networks (e.g., Tor, I2P) are insufficient for implementation in fog-based vehicular crowdsensing, since all the intermediate nodes, including vehicles and fog nodes, are curious. If the reports can be bounced between the anonymizing network's nodes before the receiving fog nodes, the property of location awareness cannot be achieved in fog-based networks. A more promising method to protect vehicles' privacy is to use anonymity techniques (e.g., pseudonyms, group signatures, and *k*-anonymity). With these anonymity approaches, the curious entities are not able to distinguish vehicles based on crowdsensing reports. However, once the crowdsensing reports are kept anonymously, no one can identify the contributors of reports, so it is difficult for the cloud to distribute benefits to the corresponding vehicles according to their distinct contributions to tasks.

Regardless of whether crowdsensing reports are delivered anonymously, customers may want to release their crowdsensing tasks without exposing their identities. The releasing tasks may contain some sensitive information from which the curious cloud can predict the reasons why customers need to issue these tasks. Therefore, how to delegate the cloud to perform the crowdsensing tasks is essential for customers with the purposes of privacy preservation and quality of service guarantees. To obtain high-quality results, one trade-off is to expose the tasks, but protect the identities instead. This scarification is acceptable for customers since the cloud cannot link the identities of customers with the contents of tasks, but accomplishes the tasks effectively. As mentioned above, the anonymity techniques (e.g., pseudonyms and group signatures) can be used to hide the customers' identities and achieve the authentication simultaneously. Nevertheless, pseudonyms need to be updated in each task, which puts a heavy burden on pseudonym management for both customers and the cloud, and group signatures are generally computationally inefficient for customers.

Fairness

Although crowdsensing services are designed as best effort services, in which the vehicles voluntarily participate to data sensing and reporting, these operations would cost storage, bandwidth, and battery of vehicles and sacrifice partial privacy about drivers. These issues may degrade the enthusiasm of vehicles for participating in tasks. One major challenge is to encourage drivers to report real-time traffic information, especially if a threat to their privacy. The best approach is to provide sustainable incentive to attract vehicles to participate in crowdsensing tasks. If the vehicles have applications with direct and indirect benefits for drivers, and strong and effective measures that protect privacy, they are easy to make contributions on data collection. In general, the more data security and benefits rewarded, the more drivers are likely to contribute to the data.

Currently, many vehicular crowdsensing applications provide direct benefits to vehicles who report traffic-related information. However, fairness is a challenge to balance, which includes two aspects: customers' fairness and drivers' fairness. In terms of the fairness of customers, the crowdsensing results acquired by customers should be worth the cost paid. The participating vehicles may be greedy for benefits and lazy in sensing. On one hand, drivers make their best efforts to offer better crowdsensing reports to earn benefits. On the other hand, drivers have an incentive to cheat in order to obtain more rewards than they fairly deserve. Vehicles may use multiple identities in disguise to report false traffic information to gain better benefits. The misbehavior of vehicles can lead to unfairness for customers, because their acquired data do not match the cost they paid for the untrustworthy crowdsensing

With these anonymity approaches, the curious entities are not able to distinguish the vehicles based on the crowdsensing reports. However, once the crowdsensing reports are kept anonymously, no one can identify the contributors of reports, such that it is difficult for the cloud to distribute the benefits to the corresponding vehicles according to their distinct contributions on tasks.

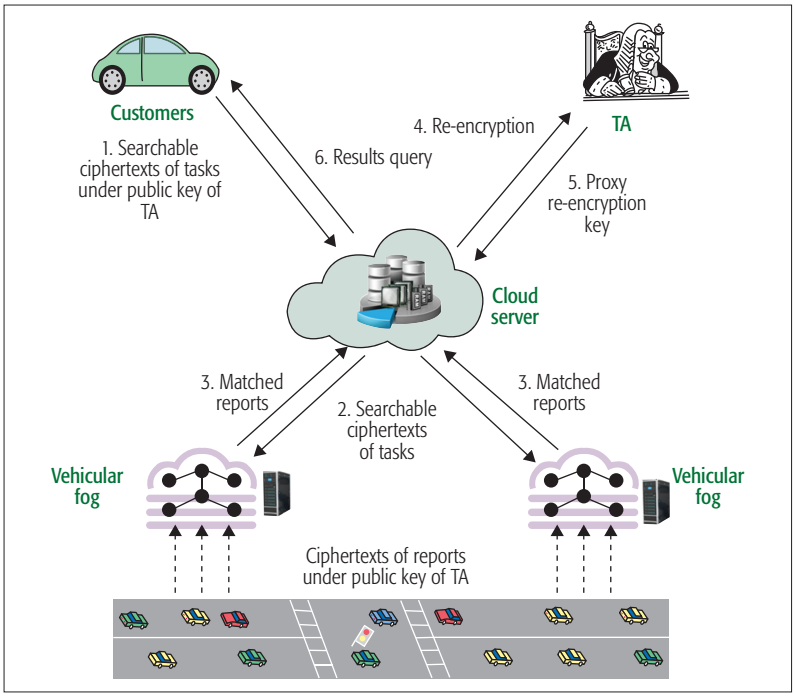

Figure 3. Model of secure tasking and reporting.

results. As a result, customers may be disappointed in the vehicular crowdsensing services, directly impacting its full flourishing.

The fairness of drivers means that the vehicles should be rewarded their deserved benefits according to their contributions to data collection. In benefits distribution, the customers determine the number of benefits that a driver should be rewarded, and the cloud is responsible for assigning the benefits to drivers. During these processes, how many benefits the drivers obtain is absolutely controlled by the customers and the cloud. Thus, the drivers may be rewarded less benefits than they fairly deserve because of customers reneging and embezzlement of the cloud. Specifically, the customers may refuse to pay the benefits or just fulfill partial benefits they promised in task releasing, and the cloud embezzles part of the benefits and only assigns the rest to the participating vehicles. This misbehavior seriously damages the enthusiasm of vehicles. Therefore, how to guarantee the fairness of vehicles is dramatically critical in vehicular crowdsensing. One possible solution is to employ a trusted third party to verify the fairness for vehicles. However, this leads to an assumption is pretty strong that there is a regulator to normalize the operations of customers and the cloud. Thus, it is necessary to design a verifiable reward distribution mechanism for vehicles to ensure their fairness.

Solutions

To address the security, privacy, and fairness challenges in FVCS, exquisitely designed protection solutions are desirable. In this section, we introduce several state-of-the-art security and privacy protection schemes for vehicular crowdsensing applications.

Secure Tasking and Reporting

In FVCS, it is critical for guaranteeing the confidentiality of both crowdsensing tasks and reports. However, there are several challenges to achieve this goal. First, once the tasks are protected, the cloud cannot retrieve the crowdsensing reports and return the results without knowing any detailed information about the tasks. Second, since customers should have the decryption capacity of the results, the retrieved crowdsensing reports should be encrypted under the public keys of the customers. Nevertheless, the vehicles are not aware of the customers when reporting. Moreover, a crowdsensing report may be shared for multiple tasks released by distinct customers. Third, when the vehicles are generating the reports, it is difficult to determine the owners of crowdsensing reports when reports are submitted, whose public keys should be used to encrypt the reports.

To overcome these challenges, proxy re-encryption [11] is promising to realize the confidentially sharing of crowdsensing reports, and searchable encryption can be used to filter the crowdsensing reports for customers. In addition, a trusted authority (TA) should be involved to achieve key management for both customers and vehicles. Specifically, the vehicles encrypt their crowdsensing reports using the public key of the TA and submit them to local fog nodes. The customers use the searchable encryption with the TA's public key to prevent their tasks from being exposed to the cloud. The cloud uses the ciphertexts of tasks to search on the fog nodes spatially located in the sensing area to retrieve the matched reports. Before returning the results to the customers, the cloud requests the TA for a proxy re-encryption key to transform the ciphertexts of reports under the public key of the TA to be the ciphertexts decryptable for the corresponding customers. Finally, the cloud generates and returns the results to the customers. As shown in Fig. 3, the proposed mechanism can solidly address the dilemma in the data collection and task execution in FVCS.

Privacy-Preserving Navigation

Vehicular crowdsensing allows vehicles to collect real-time traffic information and periodically report to fog nodes. This traffic information can be used to offer navigation service for vehicles, avoiding congestion on roads. However, when drivers are acquiring navigation results and reporting the traffic information, their privacy is inevitable to be exposed obliviously. Specifically, attackers can learn the destinations of vehicles from their navigation queries and the places frequently visited by the querying vehicles. The curious entities, including fog nodes, are able to obtain the current locations and trajectory of vehicles from the crowdsensing reports. As a result, various personal information about drivers can be predicted, such as preferences, occupation, religious beliefs, and health status. Therefore, it is of significant importance to preserve the drivers' privacy for the wide acceptance of crowdsensing-based navigation service.

In [12], Ni *et al.* proposed a privacy-preserving real-time navigation system to achieve traffic-aware navigation for drivers by utilizing vehicular crowdsensing. In the system model in Fig. 4, each vehicle registers on a TA to obtain an anonymous credential, which is a signature [13] generated by the TA. A vehicle sends a navigation query to the nearby vehicular fog, along with a group signature randomized from its anonymous credential. Meanwhile, the vehicles on roads participating in the

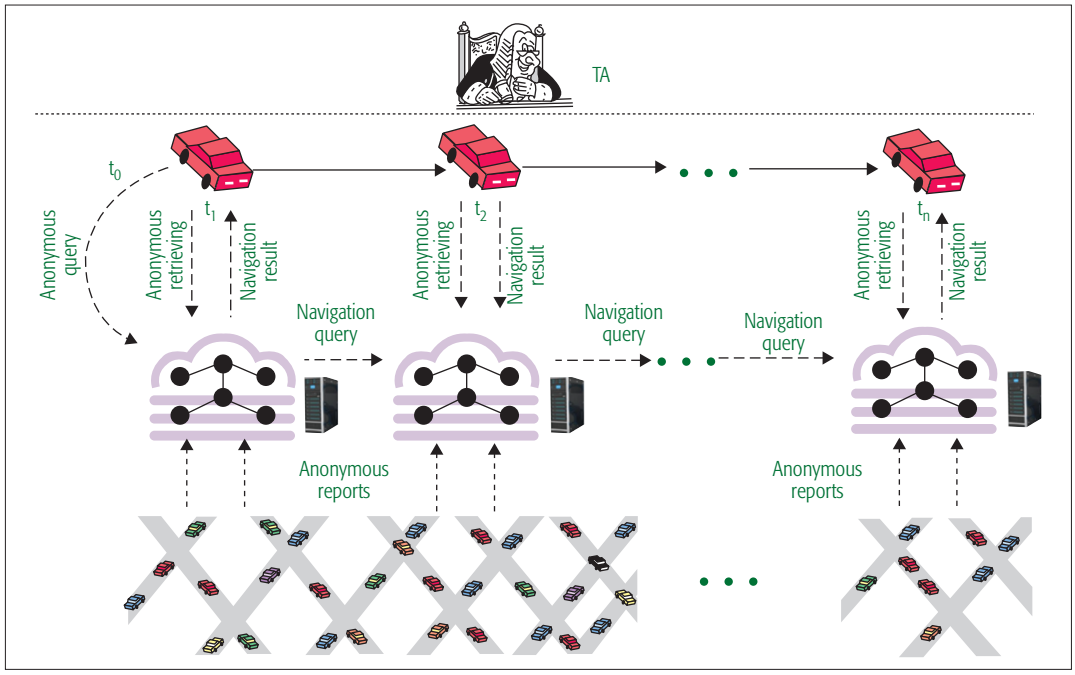

Figure 4. Model of privacy-preserving navigation.

The misbehavior of vehicles can lead to the unfairness for customers, because their acquirements do not match the cost they paid for the untrustworthy crowdsensing results. As a result, customers may be disappointed in the vehicular crowdsensing services, directly impacting its fully flourish.

crowdsensing tasks submit real-time traffic information to fog nodes without disclosing their identities through a randomizable signature generated from the anonymous credential. The fog nodes covering the location of the querying vehicle and its destination cooperatively find and return a proper path to the destination to the querying vehicle. Finally, this vehicle follows the recommended path to reach its destination. In addition, the TA can trace the identities of vehicles that misbehave to upload forged traffic information.

Secure and Deduplicated Crowdsensing

In vehicular crowdsensing, vehicles collect the traffic and road information for real-time navigation and road surface monitoring. The data sensed from the same position inevitably contain some duplicates, which may cost massive communication bandwidth and storage resources for fog nodes. A straightforward method to improve the capacity is to discard redundant copies on intermediates; however, it discloses the detailed crowdsensing reports. Data encryption provides a sophisticated approach to prevent privacy leakage, meanwhile bringing a huge obstacle to the intermediates for identifying the reduplicated reports. How to balance the contradiction between privacy leakage and data deduplication is the main challenge to achieve efficient transmission and storage of crowdsensing reports. Nevertheless, once the crowdsensing reports are deduplicated, the cloud cannot identify the contributions of participating vehicles. Although the repeated data do not improve the completeness of crowdsensing results, these redundancies can increase the results' trustworthiness, such that the contributions of the vehicles who report reduplicate data should not be ignored. In summary, it is of significance to achieve the data deduplication in crowdsensing reports without exposing the contents of reports and fairly record the contributions of vehicles.

To address these issues, Ni *et al.* [14] designed a fog-based secure and deduplicated crowdsensing framework. In this framework in Fig. 5, the fog nodes are involved to temporarily store crowdsensing reports, and realize efficient and secure data deduplication and contribution aggregation. Specifically, the vehicles encrypt their crowdsensing reports with a novel cryptographic primitive, message-lock encryption [15], where the key under which encryption and decryption are performed is derived from the message, and upload to the nearby fog node, along with key-homomorphic signatures of the reports, in which the signatures generated by different vehicles on the same messages can be aggregated to be one signature. After the fog node receives the crowdsensing reports from vehicles, it can check whether two crowdsensing reports are reduplicated without knowing the detailed contents of the reports. If yes, it keeps one copy of reduplicated reports and aggregates the signatures of these reports. In this way, the fog node only needs to store one copy of repeated data, but the contributions of all the vehicles who submit redundant reports can be identified and rewarded.

Conclusions and Future Work

In this article, we have studied security, privacy, and fairness issues in FVCS. We have proposed the architecture of FVCS and introduced some typical applications. We have also provided a comprehensive review for the requirements of security assurance, privacy preservation, and incentive fairness in FVCS. Finally, we have offered several promising approaches to deal with the security, privacy, and fairness challenges in various vehicular crowdsensing applications. For our future research, we plan to develop a suite of secure mechanisms that can not only achieve privacy-preserving and incentive-fair data collection, but also verifiable reward claiming with minimized data storage and cryptographic overhead.

For our future research, we plan to develop a suite of secure mechanisms that can not only achieve privacy-preserving and incentive-fair data collection, but also verifiable reward claiming with minimized data storage and cryptographic overhead.

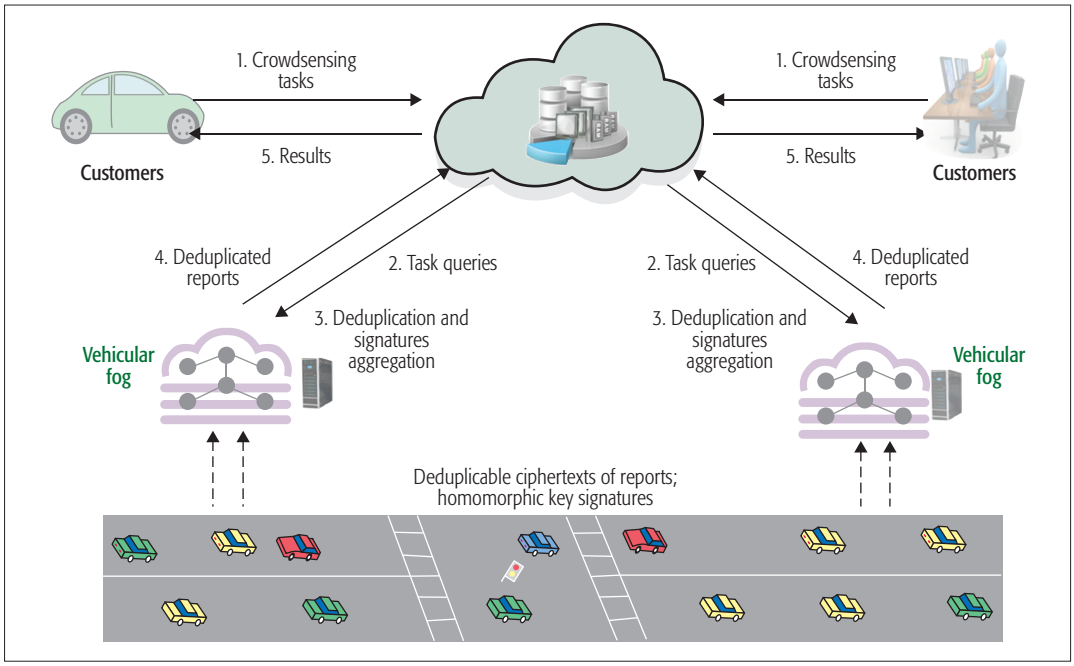

Figure 5. Model of deduplicated crowdsensing.

References

[1] R. K. Ganti, F. Ye, and H. Lei, "Mobile Crowdsensing: Current State and Future Challenges," *IEEE Commun. Mag.*, vol. 49, no. 11, Nov. 2011, pp. 32–39.

[2] K. Yang *et al.*, "Security and Privacy in Mobile Crowdsourcing Networks: Challenges and Opportunities," *IEEE Commun. Mag.*, vol. 53, no. 8, Aug. 2015, pp. 75–81.

[3] X. Lin *et al.*, "Security in Vehicular Ad Hoc Networks," *IEEE Commun. Mag.*, vol. 46, no. 4, Apr. 2008, pp. 88–95.

[4] E. Lee, M. Gerla, and S. Y. Oh, "Vehicular Cloud Networking: Architecture and Design Principles," *IEEE Commun. Mag.*, vol. 52, no. 2, Feb. 2014, pp. 148–55.

[5] L. M. Vaquero and L. Rodero-Merino, "Finding Your Way in the Fog: Towards a Comprehensive Definition of Fog Computing," *ACM SIGCOMM Comp. Commun. Rev.*, vol. 44, no. 5, 2014, pp. 27–32.

[6] J. Sun *et al.*, "SecureFind: Secure and Privacy Preserving Object Finding via Mobile Crowdsourcing," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, 2016, pp. 1716–28.

[7] S. Chen *et al.*, "Rise of the Indoor Crowd: Reconstruction of Building Interior View via Mobile Crowdsourcing," *Proc. SenSys*, 2015, pp. 59–71.

[8] H. Jin *et al.*, "INCEPTION: Incentivizing Privacy-Preserving Data Aggregation for Mobile Crowd Sensing Systems," *Proc. MobiHoc*, 2016, pp. 341–50.

[9] Z. Chen *et al.*, "A Limited Proxy Re-Encryption with Keyword Search for Data Access Control in Cloud Computing," *Proc. NSS*, 2014, pp. 82–95.

[10] K. Zhang *et al.*, "Exploiting Mobile Social Behaviors for Sybil Detection," *Proc. INFOCOM*, 2015, pp. 271–79.

[11] G. Ateniese *et al.*, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," *Proc. NDSS*, 2005, pp. 29–43.

[12] J. Ni *et al.*, "Privacy-Preserving Real-Time Navigation System Using Vehicular Crowdsourcing," *Proc. VTC-Fall*, 2016, pp. 1–5.

[13] D. Pointcheval and O. Sanders, "Short Randomizable Signatures," *Proc. CT-RSA*, 2016, pp. 111–26.

[14] J. Ni, X. Lin, K. Zhang, and Y. Yu, "Secure and Deduplicated Spatial Crowdsourcing: A Fog-Based Approach," *Proc. IEEE GLOBECOM*, 2016, pp. 1–6.

[15] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-Lock Encryption and Secure Deduplication," *Proc. EUROCRYPT*, 2013, pp. 296–312.

Biographies

Jianbing Ni [S'16] (j25ni@uwaterloo.ca) received his B.E. and M.S. degrees from the University of Electronic Science and Technology of China in 2011 and 2014, respectively. He is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research interests are applied cryptography and information security, with current focus on cloud computing, mobile crowdsensing, smart grid, and big data.

Aiqing Zhang (aiqing.zhang@uoit.ca) received her Master's degree in circuits and systems from Xiamen University, China, in 2006. Currently, she is working toward a Ph.D degree with the Department of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, China. She is also an associate professor of Anhui Normal University, China, and a visiting scholar at the University of Ontario Institute of Technology, Canada. Her research interests include wireless network security and device-to-device communications.

Xiaodong Lin [M'09, SM'12, F'17] (xiaodong.lin@uoit.ca) received his Ph.D. degree (awarded Outstanding Achievement in Graduate Studies) in electrical and computer engineering from the University of Waterloo in 2008. He is currently an associate professor of information security at the University of Ontario Institute of Technology, Canada. His research interests are in the areas of information security, privacy-enhancing technologies, digital forensics, and applied cryptography. He has won best paper awards at conferences, including ICC 2007, ICCCN 2009, BodyNets 2010, e-Forensics 2010, and SecureComm 2016. He was a recipient of a prestigious NSERC Canada Graduate Scholarships (CGS) Doctoral scholarship, and selected as a university nominee for the NSERC Doctoral Prize (Engineering and Computer Sciences category).

Xuemin (Sherman) Shen} [M'97, SM'02, F'09] (sshen@uwaterloo.ca) received his B.Sc. degree from Dalian Maritime University, China, in 1982, and his M.Sc. and Ph.D. degrees from Rutgers University, Newark, New Jersey, in 1987 and 1990, respectively, all in electrical engineering. He is a professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo. He was the Associate Chair for Graduate Studies from 2004 to 2008. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks. He was a recipient of the Excellent Graduate Supervision Award in 2006 and the Outstanding Performance Award in 2004, 2007, 2010, and 2014 from the University of Waterloo; the Premier's Research Excellence Award in 2003 from the province of Ontario; and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. He served as the Technical Program Committee Chair/Co-Chair for ACM MobiHoc '15, IEEE INFOCOM '14, and IEEE VTC-Fall '10; Symposia Chair for IEEE ICC '10; Tutorial Chair for IEEE VTC-Spring '11 and IEEE ICC '08; and Technical Program Committee Chair for IEEE GLOBECOM '07. He also serves/has served as the Editor-in-Chief of *IEEE Network*, *Peer-to-Peer Networking and Application*, and *IET Communications*. He is a registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of the IEEE Vehicular Technology and Communications Societies.