UAV-enabled Social Internet of Vehicles: Roles, Security Issues and Use Cases

Chaogang Tang[1], Xianglin Wei[2], Chong Liu[3], Haifeng Jiang[1], Huaming Wu[4], and Qing Li[5]

[1] School of Computer Science and Technology,
China University of Mining and Technology, 221116, Xuzhou, China
{cgtang, jhfeng}@cumt.edu.cn
[2] National University of Defense Technology, 410073, Changsha, China
wei_xianglin@163.com
[3] The School of Engineering and Applied Science, The George Washington University, 20052, Washington DC, United States
cliu15@gwu.edu
[4] Center for Applied Mathematics, Tianjin University, 300072, Tianjin, China
whming@tju.edu.cn
[5] Department of Computing, The Hong Kong Polytechnic University, Hong Kong, China
csqli@comp.polyu.edu.hk

Abstract. Social internet of vehicle (SIoV), also termed vehicular social network (VSN), endeavors to integrate social networking related concepts into IoV, with an aim to make vehicles capable of social communication and low-cost infotainment service provisioning. In spite of potential prospects, some issues pertaining to SIoV remain to be addressed such as security and privacy. Specifically, we in this paper propose an Unmanned Aerial Vehicles (UAVs) enabled security framework to protect the security and privacy of SIoV. On one hand, we split the evolvement of SIoV into two phases and elaborate the roles and functionalities of vehicles in each stage; on the other hand, owing to high flexibility, fast deployment, and low-cost maintainability, we incorporate UAVs into SIoV with the purpose of accomplishing multiple functions including communication range extension, data processing improvement and security protection. Use cases are also given in hope to provide some insights within UAV enabled SIoV.

Keywords: Social internet of vehicle · Security · Vehicular social network · UAV · Privacy preservation.

1 Introduction

Internet of Thing (IoT) that benefits from the development of information and communication technology (ICT) has gained widespread attention in both academia and industry, with the purpose of making everyday objects connected to Internet and interactive to each other. IoT has a wide range of applications (e.g.,

Industrial Internet of thing (IIoT) and Internet of Vehicle(IoV)) [1][2]. It further lays the foundation for smart cities [3]. For instance, as a subecosystem of IoT, IoV envisions a scenario where vehicles are the Internet enabled objects. Besides, it integrates internal vehicle network, inter-vehicle network and vehicle-mounted mobile Internet. In-car sensors are used for perceiving information related to vehicular state and the surroundings. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication technologies are needed for data delivery and information dissemination while vehicle loaded computer system enables on-site data processing and analysis. All these technologies are intended for intelligent traffic management, vehicular service provisioning, and smart vehicle controls.

Against this background, a new paradigm, named social internet of vehicle (SIoV) [4], also termed vehicular social network (VSN) [5], has been ushered in, with an aim to make vehicles capable of social communication and low-cost infotainment service provisioning, by integrating social networking related concepts into IoV [6]. VSN is stimulated by the fact that people have instinctive desires to socialize with each other, even if they are vehicle travelers on the road. To guarantee the driving safety and enjoy the driving pleasure, popular social networking software are expected to integrate into smart vehicles in SIoV, and thus people can use voice control commands to socialize with each other. Several promising technologies are pushing the social interactions on the road to shift from the smart phone centric way to the smart vehicle centric way. For example, nature language understanding (BLU), deep learning (DL), text-to-speech (TTS) technologies can be integrated to realize voice command control. Vehicular edge computing (VEC) and vehicular fog computing (VFC) [7][8] can be used for local data processing, analysis, and reasoning. These newly emerging computing paradigms become an essential part of SIoV, which helps vehicles think, act, and socialize with others link a real person. Furthermore, extensive attention has been paid to resource scheduling and allocation in the context of VEC or VFC [9][10][11]. In our previous work [7], fog computing is adopted to predict the number of parking places and realize smart parking for vehicles which try to find parking slots in peaking hours.

However, we notice that few of existing works have focused on the issues emerging along with the development of SIoV. For example, how to address the security and privacy related issues in SIoV is also a big concern in SIoV. Different from the traditional social networks, the behaviors of malicious nodes can cause immediate damages to other vehicular nodes in SIoV, e.g., communication interruption, privacy disclosure, information tamper, driving unsafe, etc. As a consequence, to address these issues, we propose a new framework called Unmanned Aerial Vehicles (UAV) enabled social internet of vehicles, where UAVs are integrated into SIoV such that UAVs can assist in security and privacy protection, data processing, and communication range extension. To be specific, the contributions of the paper can be summarized as follows:

1. We elaborate the roles and functionalities vehicles in SIoV are supposed to play and perform, respectively from different perspectives, and analyze the main limiting factors that restrict the development of SIoV.
2. A UAV enabled security framework is proposed to cope with the privacy and security related issues in SIoV. The multiple functionalities of UAVs are discussed respectively. For example, combining the advantages of UAVs, they can serve as a local authority to investigate the legality of vehicular nodes and insure the security of interactive contents among vehicles in SIoV.
3. Several use cases are given in this paper, with purpose of providing some insights within this framework.

The rest of paper is organized as follows. In section 2, we discuss the SIoV evolvement based on different stages. Section 3 introduces the commercial applications of UAVs. In section 4, we analyze the advantages from different perspectives, when UAVs are incorporated into social internet of vehicles. In section 5, two examples are given to motivate our works in this paper. Finally, the conclusion comes at section 6.

2 SIoV Evolvement

2.1 Roles and Functionalities of Vehicles in SIoV

Considering the potential benefits of SIoV, people expect that the conventional social skills and methods can be extended to the internet of vehicles [4][16][17]. Driving safety is the primary issue to be considered whenever travelers (e.g., drivers and passengers) are on the road. Currently, socializing by smart phone has become the most dominant way in daily life, especially for the younger generations. Driver distraction caused by smart phone usage has contributed to numerous traffic crashes worldwide. The need for friendly human-vehicle interactive environment, e.g., socializing by smart vehicles instead of mobile phone becomes increasingly urgent, which constantly stimulates the development of SIoV. To achieve this goal, automotive intelligence design needs to fuse BLU, DL, TTS technologies. Also, auto manufacturers gradually turn their attention to SIoV in recent years. For example, vehicular operating systems including BMW iDrive, Audi MMI, and Mercedes-Benz COMMAND have already embedded social oriented applications, and gained positive reviews from consumers.

As shown in Fig. 1, we classify the functions of intelligent vehicles into eight categories based on consumers' expectation toward what an intelligent vehicle is supposed to have. Some of these functions have already been available in vehicles while others remain the conceptual phase. For example, remote control in the category seven has been realized in most of vehicles, which style themselves as intelligent vehicles such as LYNK&CO and ROEWE from the recent rise of Chinese carmakers. Moreover, according to the characteristics of SIoV, we split the evolvement of SIoV into two different phases – human-vehicle oriented internet of vehicles and vehicle-vehicle oriented internet of vehicles, respectively. In the first phase, SIoV mainly focuses on human-vehicle oriented service provisioning.

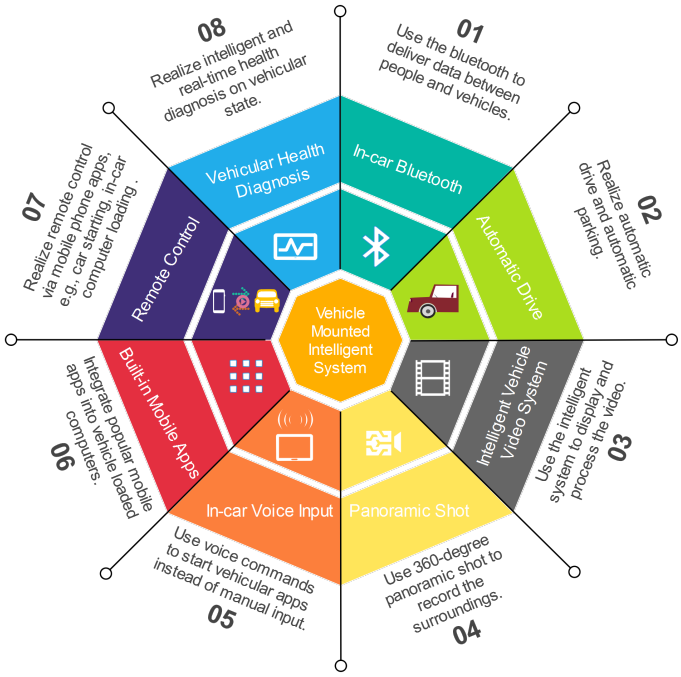

Fig. 1. Functional classification in smart vehicles

Most of functions depicted in Fig. 1 belong to this phase. People can make social connections via vehicles instead of mobile phones. However, as far as intelligence is concerned, vehicles in this stage are not smart enough to be engaged in social behaviors. It is still a challenge to integrate social networking software into vehicular operating systems, not to mention the social behaviors of vehicle.

In the second phase, interactions have already shifted from the human-vehicle way to the vehicle-vehicle way. Specifically, a comparison between the two phases from different perspectives is shown in Fig. 2. In contrast to the first phase, phase two truly realizes the social internet of vehicles. A miraculous scenario is anticipated where intelligent vehicle can think, act, and socialize with others link a real person. On one hand, interactions between people and vehicles occur frequently, which can improve the driving pleasure. Furthermore, voice control in vehicles will be the dominant way to socialize among people. On the other hand, spontaneous interactions among vehicles themselves are very common. This kind of interaction usually does not need the involvement of drivers at the beginning. People usually only need to make a decision at the end.

2.2 Security Issues in SIoV

Although the prospect of SIoV is tempting, quite a few obstacles remain to be removed from SIoV. One of big concerns is the security issue. The traditional

Features	Phase I	Phase II
Sponsor	Human	Vehicle
Terminator	Vehicle	Vehicle
Automation Degree	Low	High
Man-Machine Interaction	Low Frequency	High Frequency
Human Involvement	Not Much	Much
Safety	Low	High
Privacy	Not Safe	Safe
Social Content	Types Limited	Types Not Limited
Data Size	Avearge	Extremely Large

Fig. 2. Comparison of two phases in the evolvement of SIoV

social networks (e.g., Twitter) connect people who have known each other in the real world or are closely associated through certain social connections [4]. However, the vehicular social networks connect vehicles/drivers who are anonymous or unknown to each other beforehand. Drivers tend to trust each other, if they have similar commuter routes or the same brand of vehicles. Then, some potential common interests can be shared and disseminated in the vehicular social networks. During this process, different kinds of attacks can be launched by malicious vehicles, which undermines vehicular social networks and restricts the development of SIoV. Furthermore, these attacks can even cause life-threatening accidents. Specifically, the attack behaviors include, but not limited to:

- Denial of service (DoS) attack. It is an attack behavior that tries to make network connection malfunction, e.g., by jamming vehicular social networks using a vast amount of data and information. These irrelevant messages keep the wireless channels so busy that other legitimate vehicles cannot utilize the communication resources. Thus, data delivery and service provisioning are not available any longer in VSN.
- False message injection. Malicious vehicular node in VSN can broadcast a false message to the network for its own benefits [1]. Thus, the attacker can manipulate the traffic flow and interfere the reasoning of other vehicles, giving rise to anticipated damages to the vehicles in SIoV.
- Impersonation attack. The attacker accesses the resources of the network in the disguise of a legitimate node in VSN. Then false messages can be broadcast on the behalf of that node, which may incur life-threatening damages to drivers.
- Social trust disguise. The attacker disguises its own social trust level, with an aim to obtain the others' trust in the vehicular social network. Then, the attacker may obtain others' privacy information for their illegal benefits.

In addition to these representative attack behaviors, other forms of attack also exist in vehicular social networks [1]. Extensive attention has been focused

on vehicular networks protection such as [12][13][14]. Nevertheless, few of works have been done on the security of vehicular social networks. With the development of SIoV, the issues pertaining to security and trust become significantly important. Accordingly, in this paper we focus our attention on the UAV enabled SIoV security framework, in hope to address the aforementioned issues.

3 Commercial Applications of UAVs

UAVs have broken away the originally military application restraint and become ubiquitous in the commercial field. Specifically, the common uses for UAVs in business domain can be outlined as follows. First, UAVs can act as aerial base stations to establish wireless communication links between two entities out of each other's communication range. For instance, UAVs can be applied to the post disaster relief where the terrestrial infrastructures for communication are damaged. Second, better line-of-sight(LOS) characteristic brings about better remote sensing capability, which makes UAVs suitable for information collection and dissemination, e.g., in some harsh environments where people cannot make personal appearance. Third, a new computing paradigm termed aerial fog computing (AFC) is proposed that enhances UAV with computing capabilities, e.g., by equipping them with powerful computing facilities. As a consequence, UAV can provision computing resources such that the captured data can be processed and analyzed on site. Thus, the response latency can be reduced to a great extent in contrast to data processing in the remote cloud center.

Besides the aforementioned use cases, many efforts have also been made to realize the UAV-to-Vehicle (U2V) and Vehicle-to-UAV (V2U) communications [15]. The sensing capability can be further enhanced when Flying Ad-hoc Network (FANET) works collaboratively with Vehicle Ad Hoc Network (VANET). More important, AFC can be combined with VFC or VEC to fully exploit the idle computing resources in vicinity. For example, tasks from UAVs or vehicles can be accomplished with the aid of each other's computing capabilities. By doing so, on one hand, the response latency can be reduced because of local data processing; on the other hand, the pressure over the core network can be mitigated thanks to the reduction of task offloading via the backhaul links.

4 UAV Assisted Social Internet of Vehicles

Following the aforementioned introduction about UAV, we in this paper argue that UAV is helpful for social internet of vehicles owing to its high flexibility, fast deployment, and low-cost maintainability. To be more specific, first, UAV can seamlessly connect to the vehicular social networks. Second, UAV can fulfill the key requirements of SIoV such as low response latency and wide communication range. Third, UAVs can assist in coping with security and trust related issues in SIoV. In the next, we will detail these functionalities respectively.

4.1 Network Connectivity

Network connectivity determines the performance of network access of SIoV. And it should be the primary function for vehicles when they function as smart agents in the vehicular social network. Before socializing with each other, vehicles should have the ability to communicate with other entities at the beginning. These entities usually include vehicles and RSUs. VANET provides a foundation for the ubiquitous communications between vehicles themselves, and also between vehicles and RSUs. A variety of wireless communication technologies are available for data delivery and information sharing, e.g., 4G, WiFi, WLAN, ZigBee, Bluetooth, and dedicated short-range communication (DSRC). On another hand, with the advent of 5G technology, the communication between IoT devices will become much easier than before, for the reason that 5G supports end-to-end communications with higher data rates. All these advantages will boost the prosperity of SIoV.

However, an obvious drawback in current wireless communication technologies applied to VANET and VSN is that the communication range is limited. With the help of UAVs, the communication range can be extended. For example, an example is given in Fig. 3, where a car accident happens, however, the information about the incident cannot be disseminated due to lack of suitable relay nodes to forward the information. When UAV becomes engaged with this traffic incident, the problem can be readily solved. In this scenario, UAV can serve as a relay node to broadcast the information in real time. As a whole, UAV can boots the network connectivity of SIoV to a great extent.

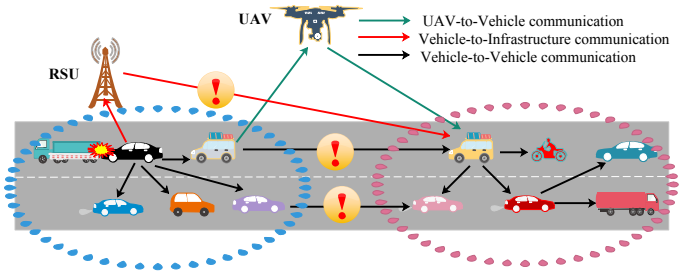

Fig. 3. An example of communication range extension using UAV[15]

4.2 Data Processing

Each vehicular node in SIoV should be equipped with powerful computing and storing resources such that they are capable of local data processing. This feature is vital to SIoV, since the "intelligence" of vehicle depends on the processing capability of vehicular brain (i.e., vehicle loaded computers). For instance, fast data processing and analysis reduces the response latency during the decision

making, which is vitally important to driving safety. Furthermore, local data processing is one of the key enablers for vehicles to logically reason, train, compute, and analyze. If these oriented tasks in application are executed at the cloud center, the response latency could be extremely long, attributed to task offloading via the backhaul links. Last, vehicles as intelligent agents can be stimulated by the potential benefits. One of these benefits is the payoff earned by contributing their computing resources. When it comes to finding a suitable scheme to fulfill these functions, VFC and VEC are proposed that fully exploit the computing capabilities of vehicles, with an aim to accomplish these goals.

On anther hand, the development of SIoV will bring about mountains of data. Of these data, some need the wireless communication resources (e.g., multimedia data sharing) while others need the computing resources such as vehicular applications and tasks. Against this background, the number of vehicular applications in SIoV is also explosively increasing. Thus, the limited computing capabilities of vehicle loaded computer systems can no longer satisfy the demands. It is not a good choice to turn to cloud computing for help as discussed above. On another hand, feasible solutions are discussed in the vehicular edge computing, where RSU connected to edge servers can act as the edge node to perform the computation tasks. Attributed to expensive deployment and maintenance, full coverage of RSU currently has not been achieved.

As a result, we in this paper argue that UAV can help turn this situation around, since UAVs equipped with powerful computing resources can constitute aerial fog computing, a new computing paradigm which can provision computing services on the wing. We believe that aerial fog computing can assist social contacts of vehicles nodes in SIoV, when tasks or applications need to be outsourced.

4.3 Security Capability

Social internet of vehicles evolves from the internet of vehicles while incorporating IoTs, machine learning, cloud computing and edge computing. Like other types of social networks, SIoV should address well the issues pertaining to security and privacy. When socializing with other entities (e.g., people, vehicles, RSUs), how to prevent and detect the attack behaviors is really one of big concerns faced by SIoV. The sensitive information may be disclosed to the malicious nodes and used for illegal benefits. Vehicular social networks are of high dynamics where vehicular nodes can join or leave for free at any time. The social information in this background is vulnerable to attacks like eavesdropping, tampering, forgery and replay. Worse still, it lacks efficient and legitimate entities to detect whether information is pushed under malicious human intervention.

Owing to the merits of UAVs, they can be very helpful for preventing and detecting the attack behaviors of malicious nodes in VSN. For example, flying above the serving area, they can collect, analyze, detect the behaviors of the vehicular nodes in SIoV, with the purpose of finding out and tracking the malicious nodes. Then the regular vehicles can be informed of the malicious ones to further isolate them. In UAV, various trustworthiness mode can be also defined such

that new security evaluation and management framework can be established to ensure the security of SIoV.

5 Use Cases

In this section, two examples are given to motivate our work in this paper.
Example 1. Traffic jam at morning peak hours annoys every driver on the road. How to avoid the traffic jam and improve the efficiency of road poses a major challenge to government as well as citizens. In the era of SIoV, we believe that the traffic jam can be mitigated dramatically. A social internet of vehicles can be established where each vehicle can independently think, socialize and reason. With the help of UAVs, global information about the traffic can be captured such as queue length, phase timing and phase sequence at each intersection. Besides, vehicular information including the destination, location, and velocity are also shared in VSN. These information is helpful for assisting decision-making. Each vehicle acting as an intelligent agent makes the best decision toward their optimization objective by reasonably adjusting the velocity, route and so on.
Example 2. Assume that there is an attacker on the road. He wants to manipulate the traffic flow by broadcasting a false car accident in VSN, and reminds other vehicles of avoidance. If the previous behaviors of this attacker are trustworthy, other vehicles may trust him this time. Then, he succeeds in manipulating the traffic flow. However, we can avoid this situation with the help of UAVs. For example, thanks to great LoS, UAVs can easily capture the picture of the road, and further judge whether a car accident exists. On another hand, UAVs can also obtain the information of passing vehicles prior to the attacker on that road and analyze their velocity and acceleration to aid the decision-making. Algorithms can also be applied to car accident detection.

6 Conclusion

Internet of Things, cloud computing, edge computing and mobile internet are considered to be the main moving forces that stimulate the development of SIoV. We in this paper envision an enticing scenario where UAVs meet the social internet of vehicles. FANET and AFC can be leveraged to assist SIoV in extending the communication range, boost the data processing abilities and improving the security. We in this paper talk about these affects from different perspectives and discuss how UAVs can seamlessly connect to SIoVs. For the further works, we plan to design efficient strategy to evaluate the trustworthiness of VSN. We also need appropriate measures to detect and track the malicious vehicles to ensure the security of SIoV during the social contacts.

References

1. Maglaras, L. A., Al-Bayatti, H. A., He, Y., Wagner, I., Janicke, H.: Social Internet of Vehicles for Smart Cities. Journal of Sensor and Actuator Networks, 5(1), 3, (2016)

2. Pandey, M.K., Subbiah, K.: Social Networking and Big Data Analytics Assisted Reliable Recommendation System Model for Internet of Vehicles, in: Internet of Vehicles – Technologies and Services – Third International Conference, Nadi, Fiji, LNCS, 149–163, (2016)
3. Bouk, S.H., Ahmed, S.H., Kim, D., and Song, H.: Named datanetworking based its for smart cities, IEEE Communications Magazine, **55**(1), 105–111, (2017)
4. Luan, T.H., Lu, R., Shen, X., Bai, F.: Social on the road: enabling secure and efficient social networking on highways. IEEE Wireless Communications **22**(1), 44–51, (2015)
5. Wu, H., Tang, H., and Dong, L.: A Novel Routing Protocol Based on Mobile Social Networks and Internet of Vehicles. in: International Conference on Internet of Vehicles, Springer, Cham. (2014)
6. Atzori, L., Iera, A., Morabito, G., Nitti, M.: The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization. Computer Networks, **56**(16), 3594-3608 (2012)
7. Tang, C., Wei, X., Zhu, C., Chen, W., Rodrigues, J.P.C.: Towards Smart Parking Based on Fog Computing. IEEE ACCESS, **6**, 70172–70185. (2018)
8. Tang,C., Wei, X., Zhu,C., Wang, Y., and Jia, W.: Mobile Vehicles As Fog Nodes For Latency Optimization In Smart Cities, IEEE Transactions on Vehicular Technology, doi:10.1109/TVT.2020.2970763, (2020)
9. Xu, C., Lei, J., Li, w., and Fu, X.: Efficient multi-user computationoffloading for mobile-edge cloud computing, IEEE/ACM Transactionson Networking, **24**(5), 279–2808, (2016)
10. Guo, J., Song, Z., Cui, Y., Liu, Z., and Ji, Y.: Energy-efficient resourceallocation for multi-user mobile edge computing, in: 2017 IEEE Global Communications Conference, Singapore, December, 1–7, (2017)
11. Hou, X., Li, Y., Chen, M., Wu, D., Jin, D., and Chen, S.: Vehicularfog computing: A viewpoint of vehicles as the infrastructures, IEEETransactions on Vehicular Technology, **65**(6), 3860–3873, (2016)
12. Kumar, N., Iqbal, R., Misra, S., Rodrigues, J.J.: An intelligent approach for building a secure decentralized public key infrastructure in VANET, Journal of Computer and System Sciences (JCSS), **81**, 1042–1058, (2015)
13. Schweppe, H., Weyl, B., Roudier, Y., Idrees, M.S., Gendrullis, T., Wolf, M., Serme, G., de Oliveira, S.A., Grall, H., Sudholt, M.: Securing car2X applications with effective hardware software codesign for vehicular on-board networks. In Proceedings of the 27th Joint VDI/VW Automotive Security Conference, Berlin, 11C12 October, (2011)
14. Lu, R., Lin, X., Liang, X., Shen, X.: A dynamic privacy-preserving key management scheme for location-based services in vanets. IEEE Transactions on Intelligent Transportation Systems, **13**, 127–139, (2012)
15. Tang, C., Zhu, C., Wei, X., Peng, H., Wang, Y.: Integration of UAV and Fog-Enabled Vehicle: Application in Post-Disaster Relief, in: 25th IEEE International Conference on Parallel and Distributed Systems, ICPADS 2019, Tianjin, China, December 4-6, 548–555, (2019)
16. Loke, S.W.: Cooperative Automated Vehicles: A Review of Opportunities and Challenges in Socially Intelligent Vehicles Beyond Networking, IEEE Transactions on Intelligent Vehicles, **4**(4), 509–518, (2019)
17. Li, T., Zhao, M., Liu, A., and Huang, C.: On Selecting Vehicles as Recommenders for Vehicular Social Networks, IEEE Access, **5**, 5539–5555, (2017)