Research Article

International Journal of Distributed Sensor Networks

International Journal of Distributed Sensor Networks
2016, Vol. 12(8)

DOI: 10.1177/1550147716662948
ijdsn.sagepub.com
SAGE

Survey on protocols and applications for vehicular sensor networks

Jaehoon (Paul) Jeong[1] and Tae (Tom) Oh[2]

Abstract

This article surveys protocols and applications for the driving safety and efficiency in vehicular sensor networks. Nowadays, most vehicles are equipped with Global Positioning System navigation systems in the form of a dedicated navigator or smartphone app. Also, the government regulation requires vehicles to be equipped with dedicated short-range communication device for the communications among vehicles or between vehicles and infrastructure for a safety purpose. Because of this trend, many applications in vehicular networks can be envisioned for the safety of drivers and pedestrians as well as driving efficiency and fuel saving. To support these applications, protocols in physical, link, and network layers are designed and tailored for the optimal performance. This article summarizes and analyzes the state-of-art articles in the protocols and applications for vehicular sensor networks in order to shed the light of research direction on the audience in vehicular sensor networks.

Keywords

Vehicular sensor networks, protocol, application, road networks, communication

Date received: 15 April 2016; accepted: 12 July 2016

Academic Editor: Pascal Lorenz

Introduction

Nowadays, vehicular sensor networks (VSNs) have become a popular research area for a variety of services in road networks, such as the driving safety and efficiency.[1–18] Vehicles play a vital role in monitoring road surfaces to detect obstacles and road hazards, and their monitoring is performed by a collection of various motion sensors (e.g., accelerometer, gyroscope, and magnetometer), obstacle detection sensors (e.g., ultrasonic and laser sensors), and camera (e.g., on-board dash camera).

For the driving safety, monitoring the road surface and identifying the road hazards are critically important, and this monitored and detected information can be shared among the vehicles to avoid possible dangerous circumstances and situations. Additionally, it is important to support instantaneous responses to dynamic road situations and neighboring vehicles through the efficient and delay-bounded data communications, and this is possible through dedicated short-range communications (DSRC),[1,2] such as IEEE 802.11p. The driving safety can be further improved by leveraging a cooperation with infrastructure nodes (e.g., road-side units (RSUs) and relay nodes (RNs))[11] and other nodes (e.g., smartphones and Internet of Things (IoT)). Therefore, implementing the sensor networks in vehicles and stationary infrastructure nodes is vital for providing the overall safety. The protocols for driving safety include media access control (MAC) protocols, data forwarding schemes, routing protocols (i.e., unicast,

[1]Department of Interaction Science, Sungkyunkwan University, Suwon, Republic of Korea
[2]Department of Information Sciences and Technologies, Rochester Institute of Technology, Rochester, NY, USA

Corresponding author:
Jaehoon (Paul) Jeong, Department of Interaction Science, Sungkyunkwan University, Suwon 16419, Republic of Korea.
Email: pauljeong@skku.edu

multicast, and broadcast), and security services (e.g., message authentication, lightweight digital signature, user identification, and malicious vehicle detection). The protocols facilitate vehicular network applications such as a collision warning system for vehicles and pedestrians.

For the driving efficiency, sensors can measure a road congestion level for the navigation purpose. Also, vehicles can share the current congestion level and the vehicles' navigation paths with the traffic control center (TCC)[14] for the real-time coordination of the navigation service. As a result, TCC performs global optimized navigation and provides updated navigation information to the vehicles to relieve the congestion level. To perform driving efficiency features, vehicular network applications include real-time coordination-based navigation, navigation-path-aware traffic signal scheduling, and the integration of navigation system and traffic signaling system.

This article surveys the two subjects of the driving safety and efficiency in the VSNs, such as protocols, applications, and security. This article summarizes and analyzes the protocols, applications, and security that were developed for the VSNs. This article assumes that IEEE 802.11p will be a main MAC protocol for DSRC in VSNs. The article is organized as follows. Section "Protocols" surveys protocols for driving safety in VSNs. Section "Applications" surveys applications for driving safety and driving efficiency in VSNs. Section "Security" considers security for VSNs. Finally, in section "Conclusion," we conclude our article along with future work.

Protocols

This section surveys the standardization and research related to the protocols in vehicular networks. The vehicular network protocols consist of the protocols in physical, link, and network layers for vehicular networks.[1–13] The physical layer protocol is for a data encoding scheme supporting different data rates by coding rate and modulation type for vehicular environments. On top of the physical layer protocol, the link-layer protocol is for a wireless channel access to accommodate the efficient sharing of wireless channels for various vehicular applications in vehicular networks. As the link-layer or network-layer protocols, we introduce broadcast schemes and data forwarding schemes, respectively. The broadcast schemes are for the rapid data dissemination among vehicles in a limited range, such as a road segment in a downtown roadway or a highway. On the other hand, the data forwarding schemes are for the data sharing among vehicles and infrastructure nodes (e.g., RSU) in a road network via multihop in terms of intersections.

Physical-layer protocol

The Institute of Electrical and Electronics Engineers (IEEE) has standardized a series of standards for wireless access in vehicular environments (WAVE) for vehicular networks, which is called IEEE 1609 series.[1,2] The standard of IEEE 1609.4 specifies multi-channel operation and MAC layer. It also specifies a WAVE stack of protocols and includes IPv6 as a network layer protocol in data plane.[3] The standard of IEEE 1609.3 specifies the management and data delivery services between WAVE devices for vehicular networking services, such as IPv6.[3] For more efficient IP networking in WAVE-based vehicular networks, VIP-WAVE in Cespedes et al.[3] proposes an extension of IPv6, such as IPv6 neighbor discovery extension, handover, mobility management, and one-hop/two-hop communications between vehicles and an RSU.

WAVE physical layer is described by IEEE 802.11p that is based on IEEE 802.11a's orthogonal frequency division multiplexing (OFDM) mechanism.[1] This OFDM supports different data rates using a combination of coding rates and modulation types.[2] The 5.9-GHz spectrum is used for WAVE, whose 75 MHz bandwidth is divided into seven channels where each channel is 10 MHz bandwidth. There are one control channel (CCH), four service channels (SCHs), and two reserved channels. CCH is used for service announcement, and WAVE short messages for safety applications. On the other hand, SCHs are used to deliver the application data using IPv6 stack as a network layer.

Link-layer protocol

The IEEE 1906.4 standard specifies the MAC layer functions, such as IEEE 802.11p.[2] The IEEE 802.11p can use either single-physical layer (single-PHY) radio or multiple physical layer (multi-PHY) radios.[3] The single-PHY lets a WAVE device exchange information only in a single channel at a time, so the single-PHY needs continuously to switch between CCH and SCHs every certain time (e.g., 50 ms) for the interoperability with multi-channel WAVE devices.[2,3] On the other hand, the multi-PHY allows a WAVE device as a multi-channel device to monitor the CCH while it can exchange data in one or more SCHs at the same time.[2,3]

The IEEE 802.11p is based on IEEE 802.11e's enhanced distributed channel access (EDCA) mechanism and is extended to accommodate the alternating operations of CCH and SCH for the single-PHY.[1,2] In EDCA, the channel access priorities are determined by the quality of services (QoS) of applications. That is, higher QoS-demanding applications can access the WAVE channels with higher probability than lower QoS-demanding applications. The major difference

between IEEE 802.11p and IEEE 802.11e is that IEEE 802.11p uses Access Category queues on a per-channel basis through channel router function (CRF).

Broadcast schemes

Based on the WAVE link-layer protocol, many broadcast protocols have been proposed for disseminating emergency notification message for driving safety.[4–6] Qayyum et al.[4] proposed a broadcast scheme called multi-point relay (MPR) to reduce the number of redundant retransmissions with the reliable message diffusion. This MPR scheme selects an optimal set of MPRs for a node x (denoted as $MPR(x)$) through a heuristic approach using the relationship of one-hop neighbors and two-hop neighbors for the node x. The optimal selection of MPRs is non-deterministic polynomial-time NP-hard. The heuristic approach tries to construct the set $MPR(x)$ such that a minimum set $MPR(x)$, which has the one-hop neighbors of the node x, can cover both one-hop neighbors and two-hop neighbors of the node x. Through simulations, the authors showed that MPR has better performance than pure flooding in terms of message diffusion speed and the number of retransmissions.

Ros et al.[5] proposed a broadcast scheme called Acknowledged Broadcast from Static to highly Mobile (ABSM) protocol for vehicular scenarios, which uses local information acquired via periodic beacon messages with acknowledgements. This scheme uses connected dominating set (CDS) for efficient message dissemination and neighbor elimination scheme (NES). CDS is constructed as a backbone network to reduce redundant transmissions in a message broadcasting. Only nodes belonging to the CDS can retransmit the broadcast message as RNs. As known, finding a minimum CDS is NP-hard, so this article proposes a heuristic method for CDS, using one-hop neighbor information acquired via beacon messages. With NES, the proposed scheme can reduce further redundant retransmissions by beacon messages, which include the identifiers of received messages. By overhearing the beacon messages from its neighbors, a node will not rebroadcast a message if all its neighbors are believed to have received the message via the previous transmissions.

Slavik and Mahgoub[6] proposed a statistical broadcast called Distribution-Adaptive Distance with Channel Quality (DADCQ) protocol. This DADCQ uses a distance method to select forwarding nodes for broadcasting. For this distance method, a value of a decision threshold determines the performance of DADCQ. However, the optimal value of such a threshold is different on scenarios, so the design of a decision threshold function for such a threshold is important. This article suggests a decision threshold function that is adaptive to the environments, such as node density, spatial node distribution pattern, and wireless channel quality. As a result, the proposed scheme can operate efficiently under various conditions. Using simulations, the authors showed that the proposed scheme achieves the high reachability and the low bandwidth consumption in various road networks, such as urban roadways and highways.

Using point coordination function (PCF) in IEEE 802.11p, Chung et al.[7] proposed a WAVE PCF (WPCF) MAC protocol, which requires a certain degree of clock synchronization across nodes. It is a PCF MAC protocol that is designed to achieve efficient vehicle-to-infrastructure (V2I) communications via RSU in traffic congested areas, such as road intersections. This WPCF can be used for sharing the mobility information of vehicles around an intersection in order to prevent the vehicles from colliding with each other at an intersection. Since WPCF neither optimizes contention period (CP) length nor utilizes concurrent transmissions in contention-free period (CFP) in IEEE 802.11p, it cannot utilize wireless channels fully to allow the vehicles to effectively share their mobility information to their relevant vehicles that can collide with them with a high probability.

Using distributed coordination function (DCF) in IEEE 802.11p along with directional antenna, Feng[8] proposed a location- and mobility-aware (LMA) MAC protocol. LMA performs a carrier sense multiple access with collision avoidance (CSMA/CA) and exponential backoff-based DCF mode for vehicular ad hoc networks (VANET). LMA allows vehicles to exchange their mobility information with their neighboring vehicles moving in the same direction with directional antenna. In highway with strip (i.e., separation barrier between two directed road segments), vehicles need to talk to their neighboring vehicles moving in the same directed road segment rather than other vehicles moving in the other directed road segment. LMA can use the predicted locations and mobility of target vehicles and perform directional transmissions by using beamforming for effective broadcast. LMA takes advantages of directional antennas for the spatial reuse of a channel by considering direction and can be extended to use transmission power control for the adjustment of the transmission range for the intended receivers.

Data forwarding schemes

This section summarizes data forwarding schemes for multihop V2I, infrastructure-to-vehicle (I2V), and vehicle-to-vehicle (V2V) communications.[9–13] According to the data forwarding schemes, it is assumed that there may be (1) RSU as an infrastructure node connected to the Internet, (2) RN as a temporary packet holder without the connectivity to the

Internet, and (3) TCC as a vehicular cloud for the networking and management of vehicles in road networks.

Zhao and Cao[9] proposed a data forwarding scheme for V2I data delivery called vehicle-assisted data delivery (VADD). VADD uses a stochastic data forwarding algorithm with a metric called expected delivery delay (EDD) from a moving vehicle to a stationary node, such as RSU. The EDD is computed on the basis of vehicular traffic statistics, such as the vehicle arrival rate and average speed per road segment along with the digital roadmaps provided by Global Positioning System (GPS) navigation systems. The goal of VADD is to minimize multihop V2I data delivery delay. The EDD from a source intersection (having a packet carrier vehicle) to a destination intersection (having an RSU) is computed using a recursive formula.[9] A road segment is defined as a link having a start intersection (i.e., entrance) and an end intersection (i.e., exit). The EDD from a link's start intersection (having a packet carrier vehicle) toward the destination intersection via the link's end intersection consists of a link delay (i.e., packet delivery delay by forward-and-carry approach over a link) and the expected sum of EDDs at the end intersection for all the possible branching cases to the neighboring intersections. However, the limitation of VADD is that it does not use the trajectories of the available individual vehicles to determine a better next-hop carrier among two physically adjacent vehicles, whose trajectories may be totally different.

Jeong et al.[10] proposed a multihop V2I data forwarding scheme called trajectory-based data forwarding (TBD) using both vehicular traffic statistics and individual vehicle trajectories. TBD improves VADD for the V2I data delivery, using individual vehicle trajectories in a privacy-preserving manner. For an extremely light traffic scenario, let us assume that the data forwarding is performed by a small number of vehicles. For the current packet carrier, assume that there are two neighboring vehicles car_1 and car_2 heading to the same intersection, which are the possible next-hop carriers in this road network. It is assumed that car_1 has a vehicle trajectory to pass through an intersection having an RSU after a short time (e.g., 5 min), but car_2 has a vehicle trajectory to pass through an intersection having an RSU after a long time (e.g., 1 h). Of course, the current packet carrier should forward its packets to car_1 having a shorter EDD than car_2. Since VADD does not utilize individual vehicle trajectories to compute EDD, it is not guaranteed that VADD selects car_1 as the next packet carrier. On the other hand, TBD allows car_1 to be selected as the next packet carrier through the individual vehicle trajectories of car_1 and car_2. Each vehicle computes its own EDD with its vehicle trajectory and vehicular traffic statistics without sharing its own trajectory with other vehicles. Since each vehicle shares only its EDD with its neighboring vehicles within one-hop communication range, the privacy information of individual trajectory is not disclosed to other vehicles.

VADD and TBD are for multihop V2I data forwarding schemes. For the bidirectional communications between a vehicle and an RSU, multihop I2V data forwarding should be supported. Jeong et al.[11] proposed a multihop I2V data forwarding scheme called trajectory-based statistical forwarding (TSF). To deliver data packets from an infrastructure node such as RSU to a moving vehicle (as packet destination), TSF requires the trajectory of the packet destination vehicle. It is assumed that the packet destination vehicle periodically reports its current position, direction, speed, and vehicle trajectory to TCC for the location management by using V2I data delivery. Note that TCC can track the future position of each registered vehicle with its vehicle trajectory. A challenge of I2V is that a vehicle as a packet destination is moving over time during the packet data delivery process, which is not like the condition of VADD and TBD such that an RSU as a packet destination is stationary. To deliver a packet from an RSU to a moving vehicle over multihop, the packet should be delivered to the location (e.g., intersection) having the destination vehicle with the temporal encounter of the packet and destination vehicle. That is, the packet delivery requires the spatio-temporal rendezvous of the packet and destination vehicle in the road network. TSF selects a target point (i.e., packet destination intersection) with a high delivery probability based on the probability distributions of the packet delivery delay from an RSU to the target point and the destination vehicle travel delay from a destination vehicle's current position to the target point. For the reliable packet forwarding from an RSU to a target point multihop away from the RSU, TSF requires RNs at intersections as temporary packet holders to forward packets to the intended direction along the packet forwarding path toward the target point. Without the RNs, the packets cannot be forwarded to the intended direction because there may be no vehicle moving to a road segment to the intended packet forwarding path.

For the efficient multihop I2V multicast in road networks, Trajectory-based Multi-Anycast forwarding (TMA)[12] was proposed, which is tailored and optimized in terms of transmission cost. TMA is an extension of TSF for the I2V multicast. TMA constructs a multicast tree whose root is an RSU as a packet source and whose leaf nodes are the target points of destination vehicles in a multicast group. Each target point per multicast group member vehicle is computed through the target point selection method of TSF. An initial multicast tree is constructed with the merging of the shortest paths from the RSU to the shortest delivery paths to the target points. It is transformed to another

multicast with lower cost through a constrained minimum Steiner tree algorithm.[12]

For multihop I2V data delivery, TSF requires RNs as infrastructure nodes, which means additional cost for infrastructure. Travel prediction-based data forwarding (TPD)[13] was proposed as a multihop I2V data forwarding scheme without RNs by fully utilizing the trajectories of vehicles in a road network, which are possible packet carriers. It is assumed that the trajectories of vehicles are maintained by TCC through the voluntary report of vehicles. With the up-to-date trajectory information, TPD can construct a forwarding sequence of packet carriers from an RSU to a destination vehicle. This forwarding sequence is executed by a predicted encounter graph whose nodes are packet carriers and whose edges indicate the encounter events of a packet carrier (as a parent node) and its next packet carrier (as a child node) with an encounter probability of the current packet carrier and its successor carrier. The encounter probability considers the encounter of two vehicles at either a road segment or an intersection. The encounter probability of the spatio-temporal rendezvous of two vehicles is computed by the probability distributions of the travel delays of these two vehicles, which are modeled as a Gamma distribution. With this predicted encounter graph, an expected delivery ratio (EDR) of a packet from a source RSU and a destination vehicle is computed via multiple intermediate packet carrier vehicles that have an encounter probability above a certain threshold (e.g., 60%).

Applications

This section describes the survey of applications for driving safety and efficiency in vehicular networks, such as navigation system, pedestrian protection system, vehicle collision avoidance (CA) system, and green driving assistance system.[14–18]

Navigation system

Jeong et al.[14] proposed an outdoor navigation system called a self-adaptive interactive navigation tool (SAINT), which is tailored for cloud-based vehicular traffic optimization in road networks. The legacy navigation systems (e.g., Waze and Tmap) guide vehicles to navigate toward their destination less effectively with only vehicular traffic snapshot. Since these legacy navigation systems provide vehicles with a per-vehicle optimized navigation path without considering the planned load balancing in road segments, they cannot provide vehicles with a navigation service to improve the overall navigation performance of all the vehicles in the road network. This is because the per-vehicle optimized navigation service may let vehicles toward the same destination take the common road segments in the road network along with their shortest travel paths, which are based on the vehicular traffic snapshot. On the other hand, to provide the load balance of the vehicles over the road network, SAINT introduced a virtual congestion metric called congestion contribution value per road segment. If many vehicles take a common road segment along their travel paths, the road segment will have a high congestion contribution. SAINT guides vehicles to take a travel path from their source position to their destination position such that the accumulated congestion contribution values of the road segments along their travel path are minimum to affect the least impact on the congestion on the road network. For the minimum congestion contribution paths, the vehicles are required to detour with a bounded distance by a certain level of sacrifice, that is, a certain extended travel time for the shortest travel time based on the snapshot of vehicular traffic statistics. Through simulations in the road map of Manhattan in New York, it is proved that SAINT can provide shorter travel time for vehicles than the legacy navigation systems, for example, the reduction in the travel delay by 19% during rush hours.

Pedestrian protection system

Hwang and Jeong[15] proposed a smartphone-based road safety app called Safety-Aware Navigation Application (SANA) for pedestrian protection in vehicular networks. This SANA assumes that a smartphone has a DSRC device for vehicle-to-pedestrian communication, which is expected to be integrated into a smartphone for Intelligent Transportation Systems (ITS) services in near future. Because of the popular usage of smartphone on streets, pedestrians may not be well-aware of the surrounding road traffic. Therefore, they are exposed to road accidents and casualties. Thus, this article proposes a smartphone app to protect pedestrians on streets by giving both pedestrians and drivers alarming messages to warn them of possible collisions. An important requirement for such an app is to provide the users with a protection service in the way of minimizing the smartphone-battery energy consumption and the frequency of false-positive alarms. SANA provides the users of the energy-efficient alarming service by performing the scheduling of DSRC devices for maximizing their sleeping time by utilizing the mobility information of the users' smartphones. It is assumed that an RSU is deployed at an intersection and the smartphones periodically report their mobility information (i.e., speed, position, direction, and trajectory) to the RSU. The RSU collects the mobility information of the smartphones under its DSRC communication coverage and performs the schedule as a middle cloud. The RSU calculates the collision possibility that a pedestrian and a vehicle will encounter spatially and

temporally by their travel delays, which are modeled by a Gamma distribution. If the collision probability is greater than a threshold (e.g., 60%), SANA generates an alarm to warn both the vehicle and pedestrian of a possible collision. SANA not only performs the optimization of a DSRC device's sleeping time but also performs the filtering of irrelevant smartphones in order to minimize false-positive alarms. Through simulations, the authors showed that SANA outperforms legacy schemes in terms of energy consumption and alarm delay (i.e., time difference between the expected alarm time and the actual alarm time).

Kim et al.[16] performed the user experience (UX) test for their depth-based alarming system for the effective alarm delivery for pedestrians. This alarming system puts its theoretical foundation on attentional network in cognitive neuroscience field, which studies the reaction of users for the generated events. The alarming system uses two-level alarms, such as a pre-warning alarm and a main alarm. The pre-warning alarm is an alarm to be generated 2 s before a main alarm in order for a smartphone user to be ready to receive the main alarm. The main alarm is an actual alarm to indicate that if a smartphone user does not follow the direction in the alarm, he or she will collide with a vehicle with a high probability. The authors developed an Android alarming app to inform a smartphone user of a possible collision in advance. For the UX test, the alarming app was evaluated with six types of alarm by using a remote control car. During the experiments, the authors measured four metrics such as response time, collision, disturbance, and satisfaction by recording and questionnaire. As a result, it was shown that among six sorts of alarm, pre-warning with colorful background was most effective to reduce a pedestrian's response time to a main warning, but transparency for background color was not useful. Through the experiments with a remote control car, it is shown that the proposed depth-based alarming system can effectively reduce a pedestrian's reaction time to a main warning message to avoid a possible accident, leading to the protection for pedestrians.

Vehicle CA system

Shen et al.[17] proposed a driving safety system called Context-Awareness Safety Driving (CASD). It is assumed that the vehicles can communicate with each other through V2V communication based on DSRC. Through this communication, vehicles can share a variety of mobility information related to driving, such as vehicle speed, position, and direction. Through this information sharing, CASD provides vehicles with a class-based safety action plan, which is based on the direction and position of their neighboring vehicles. The class-based safety actions consider three situations, such as line-of-sight unsafe situation, non-line-of-sight unsafe situation, and safe situation. In the line-of-sight unsafe situation, a hybrid take-action scheme is taken. If a driver's action fails, its vehicle will take over the driving control to minimize a possible collision. The timing for the vehicle to take over the control is an important factor for the prompt accident avoidance, which is based on an optimized threshold, considering road context information. Also, a dynamic path maneuver planning is proposed in order to avoid a crash in real time.

Green driving assistance system

Koukoumidis et al.[18] proposed a smartphone-based green driving assistance system called SignalGuru. SignalGuru leverages smartphones for collaborative traffic signal schedule advisory. SignalGuru tries to minimize the fuel consumption by frequent stop-and-go movement of the vehicles by traffic signals. A smartphone, which is mounted on the windshield inside the vehicle, periodically takes the snapshots of traffic lights by its on-board camera around intersections and shares them with other smartphones, which subscribed to the SignalGuru system for the prediction of traffic schedules. Green Light Optimal Speed Advisory (GLOSA), which is an application of SignalGuru, predicts the traffic light schedule and recommends to a vehicle its right speed to let the driver avoid a complete halt after a fast movement for fuel saving. Also, Traffic Signal-Adaptive Navigation (TSAN), which is another application of SignalGuru, can suggest an efficient detour to allow each vehicle to avoid stops and long waits at red lights ahead, leading to further fuel saving. From the experiments, it was shown that SignalGuru could allow an experiment vehicle to save fuel by 20.3% on average. The communication between the smartphone and SignalGuru system can use either cellular networks (e.g., 3G and 4G-LTE) or vehicular networks (e.g., WAVE).

Comparison of vehicular applications

We compare vehicular applications from sections "Navigation system" through "Green driving assistance system" in terms of possible advantages and disadvantages, as shown in Table 1. As shown in the table, the advantages of them are beneficial for people and the disadvantages are mainly the cost of implementation and communication of the algorithms or protocols. However, this cost is worthy of the benefits for the new, useful applications using vehicular networks. Therefore, based on the protocols for vehicular networks, many vehicular applications will be developed and deployed for the driving safety, pedestrian

Table 1. Comparison of vehicular applications.

Applications	Advantages	Disadvantages
Navigation system (e.g., SAINT[14])	The saving of travel time of drivers	The cost for implementation and communication of the SAINT algorithm
Pedestrian protection system (e.g., SANA[15,16])	The reduction in fatality in streets	The cost for implementation and communication for the SANA service along with RSU deployment
Vehicle collision avoidance system (e.g., CASD[17])	The reduction in road accidents	The cost for implementation and communication of the CASD protocol
Green driving assistance system (e.g., SignalGuru[18])	The saving of fuel	The cost for implementation and communication of the SignalGuru

SAINT: Self-Adaptive Interactive Navigation Tool; SANA: Safety-Aware Navigation Application; CASD: Context-Awareness Safety Driving; RSU: Road-Side Unit.

protection, driving efficiency, green driving, infotainment, and social networking in road networks.

Security

VANET has many advantages, but has its own set of issues such as security and privacy. Weakness in authentication can lead to malicious attacks that can cause danger to the drivers and the transportation systems.[19] Unlike wired networks that are protected by firewalls and gateways, the vehicles are exposed in public, and the attacks could come from various directions and approaches.[20] VANET is derived from mobile ad hoc networks (MANET) and many research works have already been done in MANET area. However, VANET brings unique characteristics such as high mobility and the large scale of the network.[19] Therefore, the VANET security needs to be revisited, and also novel security approaches need to be researched for the better protection of the vehicles by implementing authentication, integrity, and non-repudiation.[21,22]

Security threats

To design the security approaches for VANET effectively, general classifications of attacks need to be understood. The attacks can be classified into false information, denial of service (DoS), impersonation, eavesdropping, and hardware tampering.[19,20] The following sections explain how different attacks are applied to VANET.

False information. The false information consists of fake data, certificates, warning, and other security messages that can be sent by an attacker. The purpose of this attack is to deliver false information to control the vehicle and driver.[22] This attack can be achieved by manipulating the current message using man-in-the-middle attack, inserting fake messages during the message exchanges, and send messages, which were intercepted earlier, during later time to reroute the driving direction and/or confuse the drivers. One of the false information attacks is Sybil attack. This attack was first described by Douceur[23] and consists of sending multiple messages from one node with multiple identities. Because of a large number of identities, the surrounding vehicles will interpret that there exist a large number of vehicles in the area, and they may consider this situation as a traffic congestion. The vehicles will automatically try to seek alternative routes although there does not exist such a traffic congestion.

DoS attack. The DoS congests the network by sending a large number of packets from the malicious vehicles to the neighboring vehicles and can overload the computational resources of the neighboring vehicles. The goal of this attack is to bring down the VANET by jamming the transmission channels and overloading the network. This causes disruption in the data traffic and prevents communication between the vehicles. This is a big problem when the emergency vehicles in the area communicate with other vehicles.

Impersonation. The impersonation occurs when the hacker pretends to be an innocent vehicle or RSU and tries to insert malicious information into the network.[24] When the two vehicles communicate, the attacker as a third party, which pretends to be a legitimate vehicle, can perform man-in-the-middle and spoofing attacks as the second vehicle gains access to the messages from the first vehicle. Also, a vehicle can pretend to be an RSU to receive packets from the surrounding vehicles.

Eavesdropping. The eavesdropping considers to be a passive attack and just collects information while overhearing the vehicular communication. The information such as vehicle information and confidential data of the drivers can be used to perform offensive attacks later. It is fairly easy to collect vehicle-specific information since vehicles broadcast their information to other vehicles

and RSUs. This information can be used to target the potential vehicles that could be hacked later to obtain the confidential information such as drivers' identities and other private information.

Hardware tampering. The hardware tampering occurs when the hackers manipulate on-board hardware for their advantages and benefits. For example, the hacker can tamper with an RSU hardware to manipulate the traffic information and collect information as well. Also, the hacker can purchase an RSU to study the internal architecture of the unit and manipulate the unit to act as a legitimate RSU to perform man-in-the-middle attack for the hacker.

Security requirements

To address the various types of attacks specified in section "Security threats," security requirements for VANET are important for developing the various solutions. The articles by Samara et al.[19] and Bariah et al.[20] discussed the security issues and indicated that the primary security requirements are confidentiality, integrity, availability, and non-repudiation. Confidentiality protects the information about the drivers and vehicles and all information should be encrypted when transmitted to the other vehicles and/or RSUs. The integrity means that the messages were not altered or modified without any authorization. However, the message could be changed intentionally. The availability means that the wireless channels must be available always to allow communication between the vehicles or between the vehicles and an RSU. The non-repudiation means the ability to identify the attackers even after the attack happens. This non-repudiation prevents attackers from denying their crimes later. Along with vehicle information, such as the trip route, speed, and time, any violation will be stored in the tamper proof device so that any official authorization can retrieve the data for non-repudiation.

In addition, DoS attacks or jamming of wireless channels attacks prevent any communication in the area and this is critical when congestion and/or emergency vehicles are involved. Therefore, these security requirements should be satisfied to reliable vehicular networking among vehicles and RSUs.

VANET security approaches

VANET offers many benefits for drivers and civilians in the society. Since wireless networks are the primary way for the communication between the vehicles or between the vehicles and an RSU for information sharing, this opens many potential vulnerabilities in the network with several security attacks, such as interference, jamming, eavesdropping, and man-in-the-middle attacks.

To protect the VANET infrastructure, authentication is a common way to defend the network from hackers. Authentication is a process that ensures that the content of the messages is not altered during transmission through the message verification. In order to achieve this authentication, public key infrastructure (PKI) is a common approach and uses public and private key pairs to secure the message exchange in the network. PKI is usually effective in wired and wireless networks, but can be ineffective in VANET environment because of the high-speed mobility. Also, a long verification time can be a problem in a high-speed environment such as highway.

To enhance the security of VANET, digital signature is recommended, which requires a signature to ensure the originality which provides integrity and non-repudiation. Digital signatures are easily created and transmitted as a part of traffic load. In general, digital signatures comprise three functions which are (1) creating public and private key pairs, (2) encrypting and decrypting messages, and (3) creating and verifying the signature. However, VANET has some strict requirements of short verification time and limited computation time due to the high-speed mobility. Although there are several digital signature algorithms in the VANET research community, the selection of the algorithms is based on the performance of signature creation and verification, and the size of the key, certificate, and signature. Those algorithms can be categorized into two classes: symmetric key management and asymmetric key management.

There are a number of publications related to authentication by implementing symmetric or asymmetric key managements.[20,24] The key management deals with a secure way of generating, distributing, and storing keys. The symmetric key management uses the symmetric key cryptographies to encrypt the message. This means that the same key is used to encrypt and decrypt the messages. There are several symmetric approaches proposed so far, where the vehicles must be authenticated by the trusted authorities. However, these approaches have a scalable issue, so them is difficult to apply them to a large number of vehicles.

On the other hand, the asymmetric key authentication is widely used since separate keys are used for encryption and decryption processes. Also, the asymmetric approach is further divided into the PKI-based authentication[20] and the identity (ID)-based authentication.[24] PKI uses a pair of public and private keys to encrypt and decrypt messages to establish security. That is, the public key is used to encrypt plaintext or verify the digital signature, and the private key is used to decrypt the ciphertext or create a digital signature. Many PKI-based authentication approaches have been

proposed, but those approaches require additional traffic loads and computational overhead in order to maintain and manage the vehicular certificate and the certificate revocation list (CRL).[24] The additional traffic could cause congestion and strain in the existing network infrastructure in the high traffic scenarios, such as a metropolitan area and downtown.

As another asymmetric key authentication, ID-based authentication approaches were introduced to reduce the traffic load by using digital signature schemes.[20] These are an attractive way of adopting the authentication service for VANET. Another benefit is that the public key could be derived from public identify information such as email address, network address, user name, or any combination of these identities.

Security challenges

Although security approaches are developed, VANET still has several challenges. First, there is always a trade-off between authentication and non-repudiation versus privacy within VANET environments. Another security challenge is the significant delay and/or overhead when security is implemented[21] in vehicular networks. These security challenges need to be addressed for various VSN services.

Conclusion

This article summarizes and analyzes protocols and applications for the driving safety and efficiency in VSNs. With the asset that the vehicles are equipped with GPS navigation system and DSRC device, it is expected that many applications for vehicular networks will be developed for the safety of drivers and pedestrians and also for the driving efficiency and fuel saving. For these applications, relevant protocols should be developed in various networking layers, such as physical, link, and network layers. This article reviewed the state-of-art work in the protocols and applications for VSNs along with security issues. We believe that this article will help the audience understand the state-of-art and develop new useful applications and relevant protocols in the area of VSNs. As future work, we will survey IP-based vehicular networking for intelligent transportation systems, such as IP address autoconfiguration, vehicular network architecture, routing, and mobility management.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (2014006438). This research was supported in part by Global Research Laboratory Program (2013K1A1A2A02078326) through NRF, the ICT R&D program of MSIP/IITP (14-824-09-013, Resilient Cyber-Physical Systems Research), and the DGIST Research and Development Program (CPS Global Center) funded by the Ministry of Science, ICT & Future Planning.

References

1. Ahmed SAM, Ariffin SHS and Fisal N. Overview of wireless access in vehicular environment (WAVE) protocols and standards. *Indian J Sci Technol* 2013; 6(7): 4994–5001.
2. Morgan YL. Notes on DSRC & WAVE standards suite: its architecture, design, and characteristics. *IEEE Commun Surv Tutor* 2010; 12(4): 504–518.
3. Cespedes S, Lu N and Shen X. VIP-WAVE: on the feasibility of IP communications in 802.11p vehicular networks. *IEEE T Intell Transp* 2013; 14(1): 82–97.
4. Qayyum A, Viennot L and Laouiti A. Multipoint relaying for flooding broadcast messages in mobile wireless networks. In: *Proceedings of the 35th annual Hawaii international conference on system sciences (HICSS 2002)*, Big Island, HI, 7–10 January 2002, pp.3866–3875. New York: IEEE.
5. Ros FJ, Ruiz MP and Stojmenovic I. Acknowledgment-based broadcast protocol for reliable and efficient data dissemination in vehicular ad hoc networks. *IEEE T Mobile Comput* 2012; 11(1): 33–46.
6. Slavik M and Mahgoub I. Spatial distribution and channel quality adaptive protocol for multihop wireless broadcast routing in VANET. *IEEE T Mobile Comput* 2013; 12(4): 722–734.
7. Chung J-M, Kim M, Park Y-S, et al. Time coordinated V2I communications and handover for WAVE networks. *IEEE J Sel Area Comm* 2011; 29(3): 545–558.
8. Feng K-T. LMA: location- and mobility-aware medium-access control protocols for vehicular ad hoc networks using directional antenna. *IEEE T Veh Technol* 2007; 56(6): 3324–3336.
9. Zhao J and Cao G. VADD: vehicle-assisted data delivery in vehicular ad hoc networks. *IEEE T Veh Technol* 2008; 57(3): 1910–1922.
10. Jeong J, Guo S, Gu Y, et al. Trajectory-based data forwarding for light-traffic vehicular ad hoc networks. *IEEE T Parall Distr* 2011; 22(5): 231–238.
11. Jeong J, Guo S, Gu Y, et al. Trajectory-based statistical forwarding for multihop infrastructure-to-vehicle data delivery. *IEEE T Mobile Comput* 2012; 11(10): 1523–1537.
12. Jeong J, He T and Du DHC. TMA: trajectory-based Multi-Anycast forwarding for efficient multicast data

delivery in vehicular networks. *Comput Netw* 2013; 57(13): 2549–2563.
13. Jeong J, Kim J, Hwang T, et al. TPD: travel prediction-based data forwarding for light-traffic vehicular networks. *Comput Netw* 2015; 93: 166–182.
14. Jeong J, Jeong H, Lee E, et al. SAINT: self-adaptive interactive navigation tool for cloud-based vehicular traffic optimization. *IEEE T Veh Technol* 2016; 65(6): 4053–4067.
15. Hwang T and Jeong J. SANA: Safety-Aware Navigation Application for pedestrian protection in vehicular networks. In: *Proceedings of the 2nd international conference on internet of vehicles (IOV)*, Chengdu, China, 19–21 December 2015, pp.127–138. Switzerland: Springer.
16. Kim J, Jo Y and Jeong J. Design and evaluation of a smartphone-based alarming system for pedestrian safety in vehicular networks. In: *Proceedings of the 2nd international conference on internet of vehicles (IOV)*, Chengdu, China, 19–21 December 2015, pp.221–233. Switzerland: Springer.
17. Shen Y, Jeong J, Oh T, et al. CASD: a framework of context-awareness safety driving in vehicular networks. In: *Proceedings of the 30th international conference on advanced information networking and applications workshops—device centric cloud (DC2)*, Crans-Montana, Switzerland, 23–25 March 2016, pp.252–257.
18. Koukoumidis E, Peh L-S and Martonosi M. SignalGuru: leveraging mobile phones for collaborative traffic signal schedule advisory. In: *Proceedings of the 9th international conference on mobile systems, applications, and services (MobiSys)*, Washington, DC, 28 June–1 July 2011, pp.127–140. New York: ACM.
19. Samara G, Al-Salihy WAH and Sures H. Security issues and challenges of vehicular ad hoc networks (VANET). In: *Proceedings of the 4th international conference on new trends in information science and service science (NISS)*, Gyeongju, South Korea, 11–13 May 2010, pp.393–398. New York: IEEE.
20. Bariah L, Dina S, Ehab S, et al. Recent advances in VANET security: a survey. In: *Proceedings of the IEEE 82nd vehicular technology conference (VTC Fall)*, Boston, MA, 6–9 September 2015, pp.1–7. New York: IEEE.
21. Wagan AA and Jung LT. Security framework for low latency VANET applications. In: *Proceedings of the international conference on computer and information sciences (ICCOINS)*, Kuala Lumpur, Malaysia, 3–5 June 2014, pp.1–6. New York: IEEE.
22. Raya M and Hubaux J-P. Securing vehicular ad hoc networks. *J Comput Secur* 2007; 15(1): 39–68.
23. Douceur JR. The sybil attack. In: *Proceedings of the first international workshop on peer-to-peer systems (IPTPS)*, Cambridge, MA, USA, 7–8 March 2002, pp.251–260. London: Springer.
24. Sun J, Zhang C, Zhang Y, et al. An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE T Parall Distr* 2010; 21(9): 1227–1239.