Improving Reliability of Platooning Control Messages Using Radio and Visible Light Hybrid Communication

Susumu Ishihara
Shizuoka University
Hamamatsu, 432–8561, Japan
Email: ishihara.susumu@shizuoka.ac.jp

Reuben Vincent Rabsatt
and Mario Gerla
Computer Science Department
University of California, Los Angeles
Los Angeles, CA 90095–1596, USA
Email: {rrabsatt, gerla}@cs.ucla.edu

Abstract—Autonomous platoon control is a promising auto drive technology. It frees drivers from stressful driving task and offers comfortable car trip experience. It is also expected to contribute to energy savings. In platooning control systems, beacon messages have an important role. Each member vehicle controls its acceleration according to the information of the position, speed, and acceleration included in the beacons from 1) the leader vehicle and 2) its preceding vehicle. Since the position, speed, and acceleration of a vehicle can be observed by its direct follower vehicle using on-board sensors, the beacon for preceding vehicle is not so critical. In contrast, the beacon transmitted from the leader vehicle to the member vehicles cannot be replaced by on-board sensors and is the key factor that requires high reliability. However, radio communication from the leader to the member vehicles is vulnerable to radio jamming attacks. This paper proposes a radio and visible light communication (VLC) hybrid protocol to tackle RF jamming attacks. Simulation results show that the proposed hybrid protocol can avoid long end-to-end delay and achieve high message delivery ratio even under RF jamming attacks.

I. INTRODUCTION

Autonomous platooning control is a promising auto drive technology as well as standalone autonomous driving such as Google Self-Driving Car [1]. It frees drivers from stressful driving task and offers comfortable car trip experience. It is also expected to contribute to energy savings. So far, various projects such as [2], [3], and [4] have struggled with developing autonomous platooning systems. Fig. 1 shows a typical architecture of an autonomous platooning system based on inter-vehicular communication (IVC), or cooperative adaptive cruise control (CACC) [5] [6].

In addition to the sensor-based autonomous cruise control (ACC), in which each vehicle controls its velocity according to the distance and velocity of its preceding vehicle, vehicles in an autonomous platoon have a function to control their velocity according to the information from the leader of the platoon and the preceding vehicle. Since autonomous platoon control depends on wireless communication, its performance and safety are strongly affected by the control of message exchange in the platoon.

In typical platooning systems, the leader vehicle periodically sends its position, velocity, and acceleration to the member vehicles periodically. For example, [6] recommends information update frequency of 10Hz. In addition to position, velocity and acceleration, kinematic data of the leader vehicle would be useful. We call a message including these data a beacon message in this paper. Control of platooning systems depends on the reliability of the beacon message sent from the leader, because the information delivered by the beacon message cannot be directly monitored by platoon member vehicles. On the other hand, the position, speed, and acceleration of the preceding vehicle can be monitored by using on-board sensors, such as millimeter wave radars. Thus, wireless communication between neighboring vehicles in the same platoon for telling the position, speed, and acceleration is not indispensable [7].

In addition to guaranteeing the reliability of message exchange protocols in normal situations, prevention from attacks to the wireless communication, such as forged messages and jamming, is crucial for platooning systems. In this paper, we focus on RF jamming attacks. Today, PC-based or FPGA based software radio platforms such as GNU Radio/USRP [8] and Wireless Open-Access Research Platform (WARP) [9] are not difficult to obtain and quickly implement wireless jamming attacking tools. Puñal et al. have developed some jamming attacking tools using WARP board to evaluate the...
risk of various jamming attacking methods using real cars [10]. The risk of jamming attack is inevitable. Thus, we need countermeasures against such attacks. Even if vehicles in a platoon are under a jamming attack, the control message delivery ratio and end-to-end delivery delay have to satisfy the requirement needed for the platooning control.

In this paper, we propose a radio and visible light communication (VLC) hybrid protocol for delivering the platoon leader’s beacon messages reliably under radio jamming attacks, and evaluates the effectiveness of the protocol through simulations. Radio communications such as DSRC/IEEE802.11p [11], especially in cases with omni-directional antennas, are vulnerable to jamming attacks because anyone in the range of the radio communication can send jamming signal to the victims. On the other hand, visible light communication (VLC), which is expected to be used in vehicle-to-vehicle communications using LED tail and head lights [12], has little influence on jamming attacks because the directivity of the VLC receiver is narrow and the attackers have to point the moving victim accurately to saturate the VLC photodiode receiver with strong light. Such an attack on VLC can only be performed on a single VLC link, as opposed to all vehicles in the range in the case of RF. This implies that the impact on the overall platoon control could be minimal.

It is difficult to send messages directly from the leader to all the members in a platoon through VLC due to the sharp directivity and the vehicles’ bodies that work as obstacles. Thus, the communication from the leader to members in the platoon through VLC has to be in a multi-hop manner. If the link speed is low, the multi-hop transmission leads to long end-to-end delay. However, the delay can be reduced by forwarding the message using radio communication and VLC complementary. Of course, though the radio communication may be affected by a jamming attack, the effect can be mitigated by using VLC.

The main contributions of this paper are summarised as follows.

- We propose a radio and VLC hybrid communication protocol for platooning control messages for reliable message delivery under RF jamming attacks.
- We developed a simulation model supporting both radio communication and VLC.
- Using the simulation model, we simulated message exchanges in a platooning system under RF jamming attacks, and present the proposed protocol works effectively to improve the end-to-end delay of the leader messages to the members and the message delivery ratio.

The organization of the paper is as follows. In the next section, we show the related work on autonomous platooning and RF jamming attacks on vehicular wireless networks. Then, we show existing techniques to mitigate the effect of RF jamming attacks and methods to detect such attacks. In Section 3, we show the system model of platooning and jamming attacks we treat in this paper. Then in Section 4, we propose a radio and VLC hybrid protocol to enable reliable and fast beacon message delivery under RF jamming attacks. In Section 5, we present our simulation model that supports both radio and VLC communications on vehicles, then evaluate the effectiveness of the proposed method through comprehensive simulation. Finally, we conclude the paper in Section 6.

II. RELATED WORK

Recently, research for using VLC in vehicular networks has been active because it has the potential to realize wireless communication that is robust to RF jamming attacks with low cost devices that can be shared with illumination and visual signal systems. For example, Yu et al. propose a model for a VLC link based on measurement campaign of an experimental VLC system built with off-the-shelf LED and photo diode devices on a scooter [12]. Tomas et al. developed a simulation module of physical and MAC layers of VLC on vehicles for JiST/SWANS wireless network simulator [19].

To the best of our knowledge, this is the first paper that evaluates the effectiveness of radio and multi-hop VLC hybrid
protocol for reliable platooning control under RF jamming attacks.

III. System Model

A. Platoon Model

We adopt the platooning controller in [5]. The controller of each member of a platoon uses the speed and acceleration of the leaders and the preceding vehicle for its input. We assume that only the leader’s information has to be sent via a wireless channel because the front vehicle’s speed and acceleration can be measured by some on-board sensors such as millimeter wave radars. We assume that each vehicle is aware of its position in the platoon. We assume the communication protocols for platooning are based on the IEEE 802.11p/IEEE 1609.4 PHY/MAC. The scheduled messages will contend for the channel in a CSMA/CA fashion. According to [6] and [15], we assume the information update frequency is 10Hz.

B. Jamming Attack Models

So far various jamming attacks on wireless LAN systems have been considered. Puñale et al. implemented the following three types of RF jammers, i) Reactive, ii) Periodical, and iii) Constant Jammers on a real radio devices and measured the effect on real vehicular networks that use IEEE802.11p-compatible communication devices. The reactive jammer sends a jamming signal when it detects a radio signal of other stations so that the CSMA/CA algorithm used in IEEE802.11p does not work well. The periodical jammer sends short jamming signal periodically with short interval. Fig. 2 presents the example of the jamming signal of the periodical jammer. The constant jammer sends a jamming signal constantly.

Their experiment results show that the periodical jammer is effective even if the SINR of the jammer is small because that the automatic gain controller (AGC) cannot quickly adapt to the change of incoming signal strength and it leads to overflow of A/D converter if it has received a weak signal. To simulate this phenomenon, the wireless network simulator has a function that gives the delay of the change of AGC’s gain. In general, wireless network simulators do not have the function for simulating such a behavior. In our simulation, this function is neglected.

In this paper, we focus on the effect of the periodical jammer because [10] presented the periodical jammer is effective even if the SINR of the jammer at the receiver (victim) is small, and thus it can be a strong candidate that attackers will use.

C. Effect of Periodic Jammer

For understanding the effect of the periodic jammer, we conducted preliminary simulations using a discrete event simulator Scenargie, a product of Space Time Engineering, LLC [20]. In this simulation, we assumed that a legal sender, a receiver, and a jammer were placed as shown in Fig. 3. The sender and receiver are IEEE802.11p compliant devices and have omni-antennas. The detail of the simulation parameters are shown in Tbl. I. We changed the distances between the jammer and the sender, and one between the jammer and the receiver. In addition, we changed the idle length of the periodical jammer model. The periodical jammer model used in their experiment, jamming signal consists of a series of a 64 micro second OFDM signal and 10 micro second idle time. In our jammer model used in the simulation, we changed the length of the idle duration from 10 micro seconds to 200 micro seconds, while we used a constant signal length 64 micro seconds. The sender constantly sends packets with a 308 byte-MAC payload every 0.1 seconds.

Fig. 4 shows the results of the simulation. If the distance between the jammer and the receiver/sender is shorter than a certain distance, the packet reception ratio quickly becomes zero. There are two reasons for the low packet reception ratio. The first is that the sender cannot find the channel idle condition if the jammer is close to the sender and the idle length is short. As shown in the results of \( d_{sr} = 10 \text{m} \) case, even if the distance between the sender and the receiver is short and the SINR of the sender’s signal at the receiver is

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx power</td>
<td>20 dBm</td>
</tr>
<tr>
<td>Modulation</td>
<td>QPSK R=1/2 (6Mbit/s)</td>
</tr>
<tr>
<td>Propagation Model</td>
<td>Free Space</td>
</tr>
<tr>
<td>Fading Model</td>
<td>Nakagami ( m = 2 )</td>
</tr>
<tr>
<td>PHY/MAC Model</td>
<td>IEEE 802.11p/1609.4 single channel</td>
</tr>
<tr>
<td>Frequency</td>
<td>5.89GHz</td>
</tr>
<tr>
<td>antenna</td>
<td>Omni-directional antenna (0dbi)</td>
</tr>
<tr>
<td>MSDU size</td>
<td>308bytes</td>
</tr>
<tr>
<td>Access category</td>
<td>AC_VI</td>
</tr>
<tr>
<td>Message transmission rate</td>
<td>10Hz</td>
</tr>
</tbody>
</table>

Fig. 3. Preliminary Simulation Scenario

Fig. 2. Periodic Jammer

TABLE I
PARAMETERS OF PRELIMINARY SIMULATION
sufficiently high (the distance between the receiver and the jammer is longer than 20m), the packet reception ratio is zero if the idle length of the jamming signal is shorter than 122 micro seconds. The second reason is that the low SINR of the sender.

From the viewpoint of attackers, it is clear to use idle time shorter than 122 microseconds. Thus we use 10 microseconds idle time in our simulation for the rest of the paper.

IV. SECURING AUTONOMOUS PLATOONING SYSTEMS WITH HYBRID VEHICULAR COMMUNICATION

A. Problem Formulation

As stated above, if an autonomous platoon that depends on only radio communication is under a jamming attack, the safety and the stability of control of the platoon are posed a threat. The messages from the leader vehicle may be lost or the delivery delay become longer than the requirement of the platoon control system.

Though one hop communication from the leader vehicle to member vehicles is useful for shortening the end-to-end delay of the message, if the SINR of a jamming signal at a member vehicle is sufficiently high compared with the message signal from the leader, the member will fail to receive the message from the leader. In addition, generally-used omni-directional antenna has a vulnerability of being attacked from any directions, while it enables to transmit and receive legitimate messages from/to any directions.

On the other hand, high-frequency electromagnetic wave including visible light inherently has high directivity. Especially visible light communication (VLC) is useful because it can use LED tail and head lamps for transmission device, and thus save the device cost. The communication between two VLC nodes has to be in a line of sight. Thus, if the transmitter and the receiver of VLC signal are at the tail and head lamp of a vehicle, it is difficult to send jamming signal so that the receiver can receive the jamming signal.

In compensation for the resistance to RF jamming attacks, VLC using head and tail lamps is hard to use broadcast for delivering the leader messages to the member vehicles in one hop because the vehicle bodies block the line of sight of the VLC. Therefore, message delivery using VLC from the leader to the members has to be done in a multi-hop manner. This leads to long end-to-end delay especially when the VLC link speed is low.

The problem to be resolved by the proposed protocol is to shorten the end-to-end delay from the leader to the members in a platoon and improve the message delivery ratio by using both radio and visible light communications when the radio communication is under a jamming attack.

B. Basic Idea

The basic idea to shorten the message delivery delay under RF jamming attacks is forwarding messages from the leader by using both radio and VLC interfaces. The leader vehicle always sends its message including its ID, position, velocity, acceleration, etc., periodically via both a radio and a VLC interface. Even if a member vehicle fails to receive a message from the leader vehicle sent via its radio interface, it will be able to receive the same message via a VLC interface if the leader has sent the message via VLC and upstream vehicles forwards the message via VLC. If a vehicle receives a new beacon message of the leader, it forwards the message via both radio and VLC message. If a member vehicle receives a message with a timestamp older than the newest message that the vehicle has forwarded, it does not forward the received message.

Since the effective range of a single jammer is limited, by using both radio and multi-hop VLC, we can improve the end-to-end message delivery delay of control messages from the leader vehicle as well as improving the message delivery ratio.

C. Restraining radio-based forwarding

Forwarding messages via radio interface may increase the radio traffic even under RF jamming attacks. This may lead to further congestion of the radio link and decrease the radio message delivery ratio from the leader. For example, if ten vehicles other than a leader vehicle are in a platoon and the half of them have successfully received a beacon from the leader directly via radio interface, then five vehicles will try to forward the message simultaneously. Under RF jamming attacks, the simultaneous attempts of transmission from multiple vehicles will make the transmission more longer.

It can be reasonable to avoid the frequency that the member vehicles forward messages received from the radio interface. From this viewpoint, we adopt the following strategies.

1) Forward via RF only if VLC is faster: If a platoon adopts Forward via RF only if VLC is faster strategy, only if a member vehicles receives a beacon message via its VLC interface earlier than via its radio interface, it forwards the message via both its radio and VLC interfaces. Otherwise, it forwards the message only via the VLC interface.

The condition that a beacon arrives via its VLC interface earlier than via the radio interface implies that the RF channel is congested and many vehicles have failed to receive RF messages. Thus, the newer message should be forwarded as soon as possible. On the other hand, if a beacon message via RF arrives faster than VLC, the radio channel is not severely congested, the necessity to forward the message via RF is not high. Of course, sending a message via radio interface under a severe radio channel congestion would worsen the channel condition.

2) Always forward via RF: If a platoon adopts Always forward via RF strategy, every time a member vehicle receives a new forwarded message either from its radio or VLC interfaces, it immediately forwards the message via both its radio and VLC interfaces.

V. EVALUATION

A. Simulation Setup

To evaluate the effectiveness of the proposed method, we conducted simulations of communication for autonomous platooning under jamming attack. We assumed each platoon
TABLE II
SIMULATION PARAMETERS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vehicular size</td>
<td>$5m \times 2.5m$</td>
</tr>
<tr>
<td>Number of platoons</td>
<td>1 and $4 \times 4$</td>
</tr>
<tr>
<td>Distance between the centers of neighboring lanes</td>
<td>5m</td>
</tr>
<tr>
<td>Vehicle head-to-head distance</td>
<td>10m</td>
</tr>
<tr>
<td>Distance between platoons</td>
<td>10m</td>
</tr>
<tr>
<td>Vehicular speed</td>
<td>17.0 m/s</td>
</tr>
<tr>
<td>Beacon frequency</td>
<td>10Hz</td>
</tr>
<tr>
<td>MAC Algorithm VLC interfaces</td>
<td>ALOHA (no retransmission)</td>
</tr>
<tr>
<td>Bit rate of VLC link</td>
<td>50 kbps</td>
</tr>
<tr>
<td>Size of VLC packet</td>
<td>200 bytes</td>
</tr>
<tr>
<td>RF Tx power</td>
<td>20 dBm</td>
</tr>
<tr>
<td>RF Modulation</td>
<td>QPSK R=1/2 (6Mbit/s)</td>
</tr>
<tr>
<td>RF Propagation Model</td>
<td>Free Space</td>
</tr>
<tr>
<td>RF Fading Model</td>
<td>Nakagami ($m = 2$)</td>
</tr>
<tr>
<td>RF PHY/MAC Model</td>
<td>IEEE 802.11p/1609.4 single channel</td>
</tr>
<tr>
<td>RF Frequency</td>
<td>5.89 GHz</td>
</tr>
<tr>
<td>RF antenna</td>
<td>Omni-directional antenna (0dbi)</td>
</tr>
<tr>
<td>RF MSDU size</td>
<td>200 bytes</td>
</tr>
<tr>
<td>RF Access category</td>
<td>AC_VI</td>
</tr>
</tbody>
</table>

variants of the proposed shown in Tbl. III.

B. Simulation Results

Fig. 7 and 8 show the time series of the end-to-end delay from the leader to 5th and 10th car when there is only 1 platoon on the road and when there are four platoons on each of four lanes respectively. Fig. 9 shows the number of messages delivered to the 5th and 10th cars every one second.

In these graphs, each dot shows that the beacon message with the timestamp at the leader shown by the x-axis of the graph has been received by the 5th or 10th car. When the beacon messages are sent only via the RF interface of the leader vehicle (FFF, (a1), (b1)), we can see that messages are not received after 26 seconds. The leader vehicle approaches closest to the jammer at 29.4 sec, and the 5th and the 10th vehicles approach there at 31.7 sec and 34.7 sec. We can see that the beacon messages are not received by the vehicles during the time period centering the timing when they are at the closest point to the jammer.

TABLE III
VARIANTS OF THE PROPOSED METHOD

<table>
<thead>
<tr>
<th>Model name</th>
<th>Use VLC Forward via RF only</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use VLC</td>
<td>Use RF Forward via RF only</td>
<td></td>
</tr>
<tr>
<td>FFF</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>FTF</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>TFF</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>TTF</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>TTT</td>
<td>True</td>
<td>True</td>
</tr>
</tbody>
</table>

The simulation consists of 10 vehicles and the head-to-head distance was 10 meters. We simulated a case where only 1 platoon exists on a road and a case where there are 4 lanes and 4 platoons are on each lane. Each vehicle has an IEEE802.11p radio interface and VLC transmitter and receiver. The VLC transmitter is attached at the center of the tail of the car, and the VLC receiver is attached to the center of the head of the car. Tbl. II summarizes the simulation conditions.

To investigate the effectiveness of reducing the frequency of forwarding beacon frames by member vehicles, we used...
Fig. 7. Time series variation of end-to-end delay of leader messages (1 platoon)

Fig. 8. Time series variation of end-to-end delay of leader messages (4 × 4 platoons)
By forwarding beacon messages using RF at each member vehicle (FTF, (a2) (b2)), the number of beacon messages received by the members increases, but the end-to-end delay is long and the number of received messages during a few seconds when the vehicle at the closest point of the jammer. If the leader vehicle cannot send any beacon message due to the busy state of the RF channel caused by the jammer, the follower vehicle cannot forward the beacon message, thus the packet received by the member vehicles is still small.

By using only VLC for forwarding beacon message of the leader vehicle (TFF (a3), (b3)), the reachability of the beacon messages improves. It can be confirmed clearly in Fig. 9. However, the end-to-end delay is long for long duration, especially when the position of the vehicle in the platoon is backward and the number of platoons is large.

Using both RF and VLC for forwarding beacon messages of the leader vehicle (TTF, (a4), (b4)), the duration of end-to-end delay is shortened. When using the forward via RF only if VLS is faster strategy (TTT, (a5) ,(b5)), due to the smaller number of RF forwarding messages caused by the strategy, the end-to-end delay is longer than TTF case when the number of platoon is 1. The idea behind the strategy is to prevent congestion caused by the messages forwarded by member vehicles under RF jamming attacks. Thus, the effect of the strategy is expected to present when the number of vehicles/platoons is large. When the number of the platoon is 16 (Fig. 8), the difference between cases of TTF and TTT is very small. We cannot see neither negative impact nor positive impact of the forward via RF only if VLS is faster strategy in this case.

Note that in the simulation of in this paper, we assumed very slow VLC link (50kbps) that will be realized by today’s off-the-shelf LED and photo-diode devices. The delay factor of the system strongly is dependent on the link speed. To balance the requirement of the end-to-end delay that the platooning algorithm requires and the link speed and technology used in VLC should be carefully chosen.

VI. CONCLUSION

We proposed a radio and visible light hybrid protocol for improving the reliability of control message used in autonomous platooning systems and evaluated the effectiveness of the strategies through simulations. The simulation results show that by using both radio communication and multi-hop visible-light communication, the reliability of platooning control messages from the leader vehicle can be significantly improved and the end-to-end delay can be shortened. Future work will be more simulation with realistic scenarios that include the real platoon mobility and precise VLC communication model including the interference of VLC signals, especially in congested and/or curved lanes.

ACKNOWLEDGMENT

This work is supported by KAKENHI 15H02689.
REFERENCES


