Security Vulnerabilities of IEEE 802.11p and Visible Light Communication Based Platoon

Seyhan Ucar*, Sinem Coleri Ergen† and Oznur Ozkasap*
Department of Computer Engineering*
Department of Electrical and Electronics Engineering†
Koc University, Istanbul, Turkey
{sucar, sergen, oozkasap}@ku.edu.tr

***Abstract*—Technology brings autonomous vehicles into the reality where vehicles become capable of cruising themselves. A vehicular platoon contains autonomous vehicles organized into groups with close proximity. It is envisioned that with the increased demand for autonomous vehicles, platoons would be the part of our lives in near future. From this perspective, vehicular platoon control using current dominant IEEE 802.11p (DSRC) is an active research field. However, DSRC suffers from problems of performance degradation due to congestion, the scarcity of radio-frequency (RF) and security. Visible Light Communication (VLC), on the other hand, is a promising complementary technology with the potential to address DSRC problems. In this paper, we investigate the security vulnerabilities of hybrid DSRC-VLC platoon in the presence of outside attackers. We develop a simulation platform to realize the hybrid platoon. We demonstrate that although VLC limits the effect of adversaries, hybrid architectures still suffer from the packet falsification and replay attacks.**

I. Introduction

Traffic safety is the fundamental concern of Intelligent Transportation Systems (ITS) where the main objective is to reduce traffic accidents by providing timely and efficient data dissemination about events like accidents, road conditions and traffic jams beyond the drivers' knowledge. The lack of traffic information and slow reaction of the drivers to the events are the major causes of many traffic injuries. Vehicular Ad Hoc Network (VANET) is proposed to mitigate these problems by vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) [1] based on DSRC. In VANET, vehicles cooperatively share and collect information with each other to jointly achieve the same goal such as vehicular safety. An autonomous vehicle, on the other hand, is a new vehicular technology that offers the possibility of fundamentally changing the ITS and has the potential to substantially affect the safety in vehicular networks. Autonomous vehicles have recently gained popularity as the Google announces its self-driving car [2].

While these smarter vehicle technologies are in progress, combined function of automation such as cooperative adaptive cruise control (CACC) comes into the reality where autonomous vehicles cruise themselves by accessing each other's information. CACC is an enhanced version of adaptive cruise control (ACC) where it not only maintains a proper following distance by slowing down once it gets too close, but also allows vehicles to cooperate with each other to make a driving decision. Vehicle platooning, on the other hand, is a technique where CACC enabled vehicles are organized into groups of close following vehicles called platoon [3]. Platoons are beneficial in terms of traffic throughput and homogeneity where vehicles are traveling with small speed variations. Moreover, platoons can improve the safety of transportation through faster response to events than drivers.

Platoons consist of a platoon leader that controls the platoon and platoon followers that follow the leader via adjusting the speed. A platoon is said to be stable if the platoon followers utilize CACC to adjust the speed and distance to the leader in terms of variation over time. Platoon stability is one of the important objectives that platooned vehicles need to achieve. To accomplish stability in the platoon, different platoon management protocols are proposed [4]–[7]. Platoon systems usually adopt the current dominant vehicular RF technology DSRC for inter-vehicular communication. However, DSRC has three main problems. First, DSRC suffers from the scarcity of RF. Increased wireless data traffic from rapidly growing wireless mobile devices is creating pressure on RF spectrum. Secondly, DSRC suffers from security problems. Usage of omnidirectional antennas makes DSRC vulnerable to all adversaries within the transmission range. Third, congestion on the DSRC channel may cause packet collision. This degrades the platoon stability and ruins the platoon safety.

VLC is a promising complementary technology with the potential to address DSRC problems. VLC is a relatively new communication technology that uses modulated optical radiation in the visible light spectrum to carry digital information. VLC brings several advantages of not causing any health concern nor any electromagnetic interference, being license-free and easy integration with existing light emitting diode (LED) equipped vehicles with low-cost additional on-board units. VLC benefits from the license-free light spectrum and immunity to RF interference to achieve high data rates. Due to line-of-sight (LoS) and confinement property of light waves, VLC causes no inter-network interference. Moreover, the light directivity and impermeability of the optical signal facilitate secure communication where it is ensured that only target vehicles participate in the communication. VLC also presents some challenges due to outdoor environments such as severe weather conditions, sunlight and ambient light which may saturate the VLC receivers. Furthermore, due to the directivity of the VLC transceivers, attackers could direct strong light to

978-1-5090-5197-7/16/$31.00 ©2016 IEEE

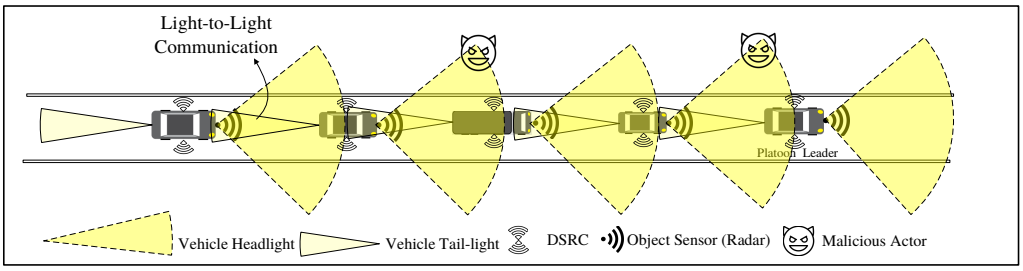


Fig. 1: Hybrid Autonomous Platoon Communication Architecture

jam the receiver which can only be performed on a single VLC link, as opposed to all vehicles in the communication range in the case of DSRC.

Many researchers have recently investigated the different characteristics of vehicular VLC such as channel characteristics [8], [9], requirements [10]–[13] and simulation models [14]. VLC is a strong candidate for platooning in hybrid architectures together with DSRC [15]–[17]. However, before the usage of VLC in a platoon, security vulnerabilities of hybrid communication need to be addressed in the presence of attacks from adversaries.

The goal of this paper is to analyze the security vulnerabilities of hybrid communication and risks associated with the attackers in the platoon. The original contribution of this paper is threefold. First, we develop a simulation platform supporting both DSRC and VLC for the hybrid communication in the platoon. Second, we analyze the platoon stability under packet falsification and replay security attacks. Third, we discuss the alternative ways to alleviate the effect of the adversary.

The rest of the paper is organized as follows. Section II describes the platoon model and attack scenarios. Section III presents the performance evaluation of platoon in the presence of attacks. Finally, conclusions and future work are given in Section IV.

II. System Model

A. Platoon Model

Fig. 1 represents DSRC and VLC hybrid communication based platoon model. Platoon members use object sensors to detect the object and vehicles in front. DSRC and VLC are used for communication between vehicles. Each vehicle cooperatively exchanges messages with its preceding and following vehicles via sending the same packet synchronously from both DSRC and VLC to achieve the CACC. Platoon communication refers to the dissemination of leader information to the platoon followers. Platoon data contains platoon identifier, the speed, position, acceleration of the platoon leader and is periodically disseminated to the platoon followers. From platoon stability perspective, platoon data needs to be delivered to the followers without any disturbance. For vehicular VLC, each vehicle contains transmitter units (TRx) and photo-diode based receiver unit (Rx) on both the front and the rear of bumpers. The LED headlights and tail-lights of the vehicle are connected to TRxs. The transmission range of tail-lights is smaller than that of vehicle headlights. Sending messages from platoon leader to all members via VLC is not possible due to directivity and other vehicles as obstacles. Thus, the data from leader to members are disseminated by the headlight and tail-light in a multi-hop manner through VLC.

B. Malicious Actor Behaviour

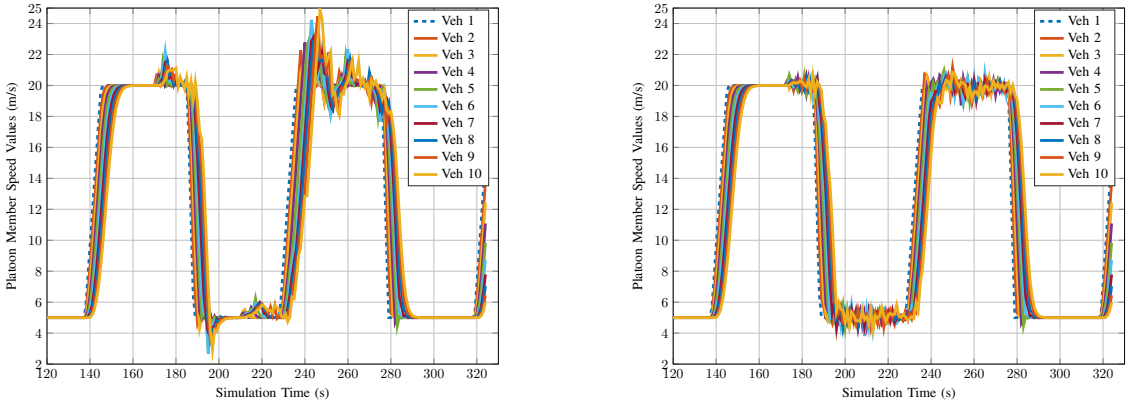
Malicious actors are equipped with both DSRC and VLC devices to prevent platoon communication. Malicious actors can be roadside units or vehicles outside the platoon. The attack scenarios are as follows.

- Packet Falsification: The adversary constantly listens to the channel for platoon communication. Upon receiving a packet, it alters the content and rebroadcasts it as if the packet comes from platoon leader. The experimental security analysis of modern automobile shows that adversaries can analyze the content of data packets using an automotive diagnostic tool [18]. For instance, consider a scenario where malicious actor changes the acceleration of platoon from slowing down to speeding up. Modifying the acceleration may result in a collision.
- Replay Attack: A platoon member controls the data packet based only on the unique platoon identifier which makes replay attack possible. An attacker can retransmit a valid data packet, masquerading as a legitimate platoon member. In this attack, the adversary overhears the platoon communication and stores the packets that are forwarded by platoon members. At a later time, it tries to replay the packets as if packets are newly generated. The replayed packet may contain out-of-date information, which misleads the platoon members and degrades the platoon stability.

In the system model, we assume that malicious actors are outside attackers and the aim of the attackers is to ruin the platoon stability and cause a collision without being a victim of it. The case where the adversary is a platoon member, on the other hand, necessitates misbehavior/anomaly detection schemes such as [19] which require multiple sources of data and a voting procedure. From this perspective, insider attacker is outside the scope of this paper.

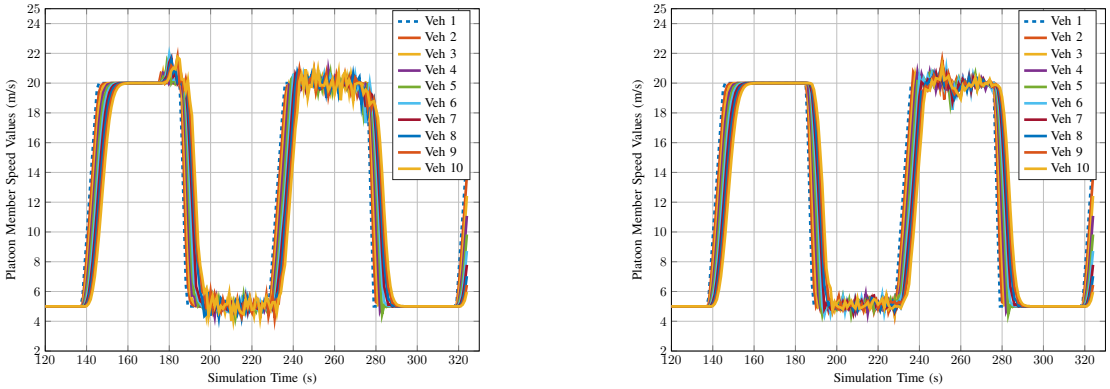
III. Performance Evaluation

The goal of the simulation is to analyze the security vulnerabilities of the pure DSRC and DSRC-VLC hybrid platoons. Platoon tries to adjust the speed to the leader by using a predefined platooning setting that consists of minimum, intended and maximum speed, maximum acceleration/deceleration and minimum space gap. In the simulation, a platoon that consists



(a) (b)

Fig. 2: Packet Falsification Attack on Platoon (a) DSRC (b) DSRC-VLC



(a) (b)

Fig. 3: Replay Attack on Platoon (a) DSRC (b) DSRC-VLC

of 10 autonomous vehicles is travelling in the leftmost lane. The first vehicle (platoon leader) is referred as $Veh1$ and shown with a dashed blue line in the graphs. Platoon members change the speed between the minimum and intended speed without exceeding the maximum value while obeying the maximum acceleration/deceleration. The analysis of security vulnerabilities is evaluated based on the speed fluctuation of platoon members over time. Attackers try to manipulate the acceleration field in packet falsification as follows. Whenever vehicles decelerate, adversaries manipulate the packet as if vehicles accelerate and vice versa. In the replay attack, on the other hand, adversaries overhear the platoon communication and store the forwarded packets. Five seconds later, stored packets are replayed to attack platoon stability.

We use VEhicular NeTwork Open Simulator (VENTOS) [20] for performance evaluation. VENTOS is an integrated simulator containing the realistic mobility generator, Simulation of Urban Mobility (SUMO) [21], discrete packet-level simulator, OMNET++ [22] and V2V communication platform, Vehicles in Network Simulation (Veins) [23]. VENTOS provides a platform to perform simulations under different speed profiles where autonomous vehicles utilize V2V communication to achieve CACC. To enable vehicular VLC, VENTOS is combined with the VLC channel model developed in [13], in which vehicular VLC is tested empirically on a vehicle with LED head and tail-lights. This model considers the inter-vehicular distance, obstacles during the movement and bearing angle of vehicles to compute the received signal strength (RSS). If vehicles are in LoS and computed RSS is larger than the VLC packet sensitivity then the packet is assumed to be received successfully by the vehicle. Table I summarizes parameters used in the experimental study.

TABLE I: Parameters

	Parameter	Value
Simulation	Simulation Time	325 s
	Vehicle Length	5 m
	Number of Vehicles	10
	DSRC Range	300 m
	Communication Frequency	10 Hz
VLC	Headlight Range	100 m
	Angular Headlight Range	-45° $\sim$ 45°
	Tail-light Range	50 m
	Angular Tail-light Range	-60° $\sim$ 60°
	Transmit Power	-60 dB
	Packet Sensitivity	-114 dB
CACC	Minimum Speed	5m/s
	Minimum Space Gap	2 m
	Intended Speed	20 m/s
	Maximum Speed	30 m/s
	Maximum Acceleration	3 m/s^2
	Maximum Deceleration	5 m/s^2
	Platoon Size	10

Fig. 2 demonstrates the speed profile of the platoon with

DSRC and DSRC-VLC under packet falsification. At $t = 172$ s vehicles enter the DSRC coverage of adversaries and exit at $t =$280 s. Fig.2-a shows that the pure DSRC get excessively affected by the attack. Speed value of platoon can fluctuate from 20 m/s to 25 m/s due to manipulated acceleration field in packet falsification. Fig.2-b, on the other hand, shows the performance of the DSRC-VLC hybrid platoon. Compared to DSRC, the hybrid platoon has small fluctuation in speed. The main reason behind this is VLC directivity, which limits the VLC range of adversaries. When vehicles are under packet falsification attack, VLC forwards the correct packet, which reduces the effect of the attack. However, when the platoon is in both DSRC and VLC coverage of adversaries (between $t =$ 200 s and $t =$220 s) the speed again shows various fluctuation. Due to the fact that, the platoon has no security protection, it accepts the falsified packets and uses them for CACC. This justifies the development of a security platoon for DSRC-VLC hybrid communication.

Fig.3 shows the speed profile of platoon with DSRC and DSRC-VLC under replay attack. Fig.3-a shows that DSRC is highly vulnerable to a replay attack. Replayed packets contain out-dated information, which disturbs the platoon stability. On the other hand, Fig.3-b shows that hybrid DSRC-VLC has less fluctuation compared to DSRC due to the directivity of light. Moreover, the replay attack is performed after five seconds where the platoon members are out of VLC range of adversary. However, the adversary can still receive the packets in the hybrid platoon due to the lack of a security protocol.

On the other hand, to mitigate the effect of adversaries, one solution can be downgrading to ACC mode when the platoon is under attack. ACC works with the larger gap and delay setting between platoon members to prevent the possible collision. However, ACC diminishes the impact of CACC driving which degrade the platoon homogeneity.

IV. Conclusion and Future Work

We investigate the security vulnerabilities of DSRC-VLC platoon and risks associated with the outsider adversary in the platoon. We develop a simulation platform to simulate the hybrid communication. We show that despite the reduction of the effect of the adversary on the platoon stability, hybrid architectures still suffer from the packet falsification and replay attacks. Due to the lack of security protocol, vehicles can be subject to modified packets in packet falsification, which disturbs the stability of the platoon. Moreover, replay attack misleads the platoon members and results in platoon instability.

Future work will concentrate on designing a secure DSRC-VLC hybrid platoon communication protocol robust to several attacks including packet falsification, replay, jamming, membership falsification and hijacking. Such a protocol requires enhancing the VLC with a secret key establishment to achieve the confidentiality, utilizing a membership verification technique to validate platoon member authentication and adopting a key management mechanism to provide key freshness.

References

[1] S. Ucar, S. C. Ergen, and O. Ozkasap, "Multihop-Cluster-Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2621–2636, April 2016.

[2] "Google Blog," https://goo.gl/hWU0V0.

[3] J. Ploeg, E. Semsar-Kazerooni, G. Lijster, N. van de Wouw, and H. Nijmeijer, "Graceful Degradation of Cooperative Adaptive Cruise Control," *IEEE Transactions on Intelligent Transportation Systems*, Feb 2015.

[4] M. Amoozadeh, H. Deng, C.-N. Chuah, H. M. Zhang, and D. Ghosal, "Platoon management with cooperative adaptive cruise control enabled by VANET," *Vehicular Communications*, 2015.

[5] S. Santini, A. Salvi, A. S. Valente, A. Pescap, M. Segata, and R. L. Cigno, "A consensus-based approach for platooning with inter-vehicular communications," in *IEEE Conference on Computer Communications (INFOCOM)*, April 2015.

[6] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, "Is Your Commute Driving You Crazy?: A Study of Misbehavior in Vehicular Platoons," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2015.

[7] M. Segata, B. Bloessl, S. Joerer, C. Sommer, M. Gerla, R. L. Cigno, and F. Dressler, "Toward Communication Strategies for Platooning: Simulative and Experimental Evaluation," *IEEE Transactions on Vehicular Technology*, Dec 2015.

[8] Z. Cui, C. Wang, and H. M. Tsai, "Characterizing channel fading in vehicular visible light communications with video data," in *Vehicular Networking Conference (VNC), IEEE*, 2014.

[9] P. Luo, Z. Ghassemlooy, H. L. Minh, E. Bentley, A. Burton, and X. Tang, "Performance analysis of a car-to-car visible light communication system," *Appl. Opt.*, Mar 2015.

[10] S. Ucar, B. Turan, S. Coleri Ergen, O. Ozkasap, and M. Ergen, "Dimming Support For Visible Light Communication in Intelligient Transportation and Traffic System," in *Urban Mobility and Intelligient Transportation System (UMITS), IEEE/IFIP Network Operations and Management Symposium (NOMS)*, 2016.

[11] B. Turan, S. Ucar, S. Coleri Ergen, and O. Ozkasap, "Dual Channel Visible Light Communications for Enhanced Vehicular Connectivity," *Vehicular Networking Conference (VNC), IEEE*, 2015.

[12] M. Abualhoul, M. Marouf, O. Shagdar, and F. Nashashibi, "Platooning control using visible light communications: A feasibility study," in *Intelligent Transportation Systems - (ITSC), 16th International IEEE Conference on*, Oct 2013.

[13] H.-Y. Tseng, Y.-L. Wei, A.-L. Chen, H.-P. Wu, H. Hsu, and H.-M. Tsai, "Characterizing link asymmetry in vehicle-to-vehicle Visible Light Communications," in *Vehicular Networking Conference (VNC), IEEE*, Dec 2015.

[14] B. Tomas, H. M. Tsai, and M. Boban, "Simulating vehicular visible light communication: Physical radio and MAC modeling," in *IEEE Vehicular Networking Conference (VNC)*, Dec 2014.

[15] S. Ishihara, R. V. Rabsatt, and M. Gerla, "Improving reliability of platooning control messages using radio and visible light hybrid communication," in *Vehicular Networking Conference (VNC), IEEE*, Dec 2015.

[16] M. Segata, R. L. Cigno, H. M. M. Tsai, and F. Dressler, "On platooning control using IEEE 802.11p in conjunction with visible light communications," in *12th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, Jan 2016.

[17] A. Bazzi, B. M. Masini, A. Zanella, and A. Calisti, "Visible light communications as a complementary technology for the internet of vehicles," *Computer Communications*, 2016.

[18] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in *Proceedings of the IEEE Symposium on Security and Privacy*, 2010.

[19] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Vehicular security through reputation and plausibility checks," *IEEE Systems Journal*, June 2014.

[20] "Vehicular Network Open Simulator (VENTOS)," http://goo.gl/OueFkO.

[21] "Simulation of Urban MObility (SUMO)," http://sumo.sourceforge.net/.

[22] "OMNET++ Networ Simulator," https://omnetpp.org/.

[23] "Vehicles in Network Simulation (Veins)," http://veins.car2x.org/.