JOURNAL OF SCIENCE
SAKARYA UNIVERSITY

Sakarya University Journal of Science

ISSN 1301-4048 | e-ISSN 2147-835X | Period Bimonthly | Founded: 1997 | Publisher Sakarya University | http://www.saujs.sakarya.edu.tr/en/

Title: CSK based on Priority Call Algorithm for Detection and Securing Platoon from Inside Attacks

Authors: Mohammed AL SHEIKHLY, Sefer KURNAZ
Recieved: 2020-01-04 17:30:13

Accepted: 2020-07-08 02:35:10

Article Type: Research Article
Volume: 24
Issue: 5
Month: October
Year: 2020
Pages: 936-947

How to cite
Mohammed AL SHEIKHLY, Sefer KURNAZ; (2020), CSK based on Priority Call Algorithm for Detection and Securing Platoon from Inside Attacks. Sakarya University Journal of Science, 24(5), 936-947, DOI: https://doi.org/10.16984/saufenbilder.670273
Access link
http://www.saujs.sakarya.edu.tr/en/pub/issue/56422/670273

Sakarya University Journal of Science 24(5), 936-947, 2020

CSK based on Priority Call Algorithm for Detection and Securing Platoon from Inside Attacks

Mohammed AL-SHEIKHLY*[1], Sefer KURNAZ[2],

Abstract

The platooning is an emerging concept in VANETS that involves a group of vehicles behaving as a single unit via the coordination of movement. The emergence of autonomous vehicles has bolstered the evolution of platooning as a trend in mobility and transportation. The autonomous vehicles and the elimination of individual and manual capabilities introduces new risks. The safety of the cargos, passenger and the advanced technology had increased the complication of the security concerns in platooning as it may attract malicious actors. In improving the security of the platoon, the threat and their potential impacts on the vehicular systems should be identified to ensure the development of security features that will secure against the identified risks. In this paper, two critical types of security breaches were identified those are Sybil attack and Delay attacks. Those security attacks can be somewhat disruptive and dangerous to the regular operation of the platoon leading to severe injuries, increased fuel consumption and delay the performance of the network. The research in this paper focuses on design, detection and the mitigation of attacks in a vehicle platoon. priority call algorithm in combination with color-shift keying modulation is used to protect the platoon alleviating the undesirable impacts such as collisions, oscillations and disintegration in the platoon caused by the attacks.

Keywords: VAENT, Priority call, Color-shift keying, Inside and Outside Attacks.

1. INTRODUCTION

With the increasing of traffic accident caused by human error that take millions of lives, recent studies showed that 60% of these accidents could be avoided if the driver had been warned half a second before the accident occur, for that it become essential to implement intelligent transportation system to reduce not only the accident that caused by human error but also to reduce pollution and traffic congestion for more safety and road efficiency [1]. Autonomous vehicles consider the future of the transportation system, where vehicles will be able to take

* Corresponding Author: mohbar.is1@gmail.com
[1] Altinbas University, Electrical and Electronic Engineering, İstanbul, Turkey.
ORCID: https://orcid.org/0000-0003-4694-152X
[2] Altinbas University, Computer Engineering, İstanbul, Turkey. E-mail: sefer.kurnaz@altinbas.edu.tr
ORCID: https://orcid.org/0000-0002-7666-2639

decision and communicate with each other to share sensitive information such as accident warning, intersection warning and blind spot warning etc, even in bad weather without human intervention. Autonomous vehicles depend on the real time exchange of sensory data for decision making, for that communication system is a major part to achieve autonomous vehicles (self-driving vehicles). vehicular ad-hoc network (VANET) which is a network design to meet the requirement of autonomous vehicles by allowing vehicles approximately 300 meters from each other to communicate and share different kind of information for instance when accident is detected, vehicle will send this information to other vehicles in the same roads to avoid it [2]. In VANET there are sub network called platoon that consist of platoon leader any many other followers for more reliability and road safety in which all the vehicles in the platoon will have same speed, acceleration, inter vehicles distance and same destination, etc. In the same platoon vehicles will share its own information with other members but the platoon leader only has the ability to take decisions in the platoon. In each platoon there are two communication (internal and external), in which internal communication called vehicle to vehicle communication (V2V) where vehicles communicate with each other in the road and external communication with road side unit known as vehicle to infrastructure communication (V2I), in which the infrastructure will provide the vehicles with road condition and weather condition, etc [2]. The most important issue that facing such a network is its security, where it's essential that this network safe from different types of attacks, whether these attacks where passive or active attacks [4]. Currently, technologies such as IEEE 802.11p suffer from many weaknesses for its latency and wide coverage area that make it vulnerable to attacks [5]. to overcome this problem visible light communication (VLC) consider proper solution due to the directionality of the communication that this technology provides which make it difficult to interrupt by an outsider malicious actor and for much higher data rate that required by vehicular system [6]. In vehicular system there are two types of attacks inside attacks and outside attacks. In term of inside attacks which count the most significant and critical attacks for such a network since one of the platoon members is the malicious actor meaning that this attacker able to send fake message from a trust member. In term of outside attacks, the attacker is an outsider meaning that the malicious actor is a vehicle near the platoon but not part of the platoon.

VANETs purpose of improving the protection of the highways, stopping collisions, supporting the passengers and help vehicles to interact with other vehicles [7]. VLC is a new technology that can overcome these attacks. problem of collaborative driving for vehicles platoon in the existence of message falsification vulnerability and communication weakness on wireless vehicular networks is investigated [8]. To secure the communication between vehicles new technology called VLC was proposed, to carry the digital information in wireless manner it will use modify light radiation in the visible light spectrum. VLC transceiver use LED to send the information and CMOS or diode image for the receiver. Improving safety performance and its long service, LED become common in automotive lighting. Similarly, many vehicles use CMOS for tracking purposes and parking assist. Previous studies have focused on VLC vehicle connections on derivation of channel characteristics [9], requirements [10][11], advanced modification schemes [6][12]. Few studies focus only on VLC security, but for non-vehicle scenarios [13].

Other studies focus on making independent vehicles more reliable and support decision-making by referring to the confidence system while integrating the maneuver scenario into the platoon. Vehicles that want to join the platoon and the relationship between platoon members have been described in the case of priority and speed adjustment but not in the security situation [14].

In [15] proposed a scheme not for eliminate the sybil attack but only to suppress the attack based on signal strength distribution. This study shows that verification error rate significantly reduced. In [16] proposed detection scenario for sybil attack based only on road side unit. This study shows that this method enormously decreases the effect of Sybil attacks. This study did not take in consideration the inside attack where the

malicious actor is not an outsider vehicle but as a vehicle part of the platoon.

Delay attack is one of the most serious attack that reduce the stability of the platoon due to the necessity of real time exchange of sensory data by adding extra time slot to the message. In [17] proposed delay attack detection based on intrusion detection system (IDS), in which sensors will observe the network by illegal listening to the transmission of its neighbors. But this detection system designed for a specific topology and their appropriate reconfiguration for various purposes or topologies is not discussed. In [18] a misdirection attack and topologies analysis were investigated where the attacker (malicious actor) will misdirect the packet to another vehicle to affect the stability and reduce efficiency due to the high delay caused by this attack. The study shows that wireless sensor network (WSN) performance in tree topology better than mesh topology.

This paper aim to detect and secure the platoon from inside attacks in particular (sybil and delay) attacks. To design secure platoon, we introduced the possible instances of attacks which can be implemented by malicious actors to exploit the weaknesses in the visible light communication algorithm used in the platoon. In securing the platoon, we explored the ability of the attacker to disrupt the traditional performance of the platoon via the control of the vehicles and modification of the control law. Further, a detection algorithm is proposed to isolate the attacker in the platoon as the first step towards mitigation of the control law. Ultimately, a priority call algorithm in combination with color-shift keying modulation is used to protect the platoon alleviating the undesirable impacts such as collisions, oscillations and disintegration in the platoon caused by the attacks.

The rest of this paper is organized as follows. Section II describes the system model in term of the platoon and attacker formation. Section III presents our result in term of detecting and securing the platoon from those attacks. Finally, concluding remarks given in Section IV.

2. SYSTEM MODEL

This section will evaluate the two internal integrity attacks i.e. Sybil and delay attack. The two attacks have been evaluated in the previous section and they tend to affect the vehicular ad hoc networks (VANET) especially in the platooning of vehicles. The design will provide the structure and communication of the platoon and the simulation design of the attacks and the solution.

2.1. Platoon Model

The structure of the platoon will be based on the following spatial position and functionalities where the vehicles can be classified into the following important roles as illustrated in the "Fig. 1". The behavior of vehicles in the Platoon in this model will not only rely on their driver's objectives but also consider the management and constraint from the Platoon control center i.e., the leader vehicle [19]. Remember vehicles will transmit request messages in case the driver wants to alter the driving behavior to match up with its own need such as arrest or destination. This characteristic will be vital in case of attacks especially internal breaches [20]. Upon reception of the request the leader will make judgement based on the condition of the traffic at the time of request. In case the leader vehicle responds to the request then all the vehicles in the Platoon will have to adjust their behavior to align with the new instructions to maintain stability in the platoon. Thus, considering the dynamics of the vehicle in the platoon then the control law may be used to describe the relationship in the platoon using the following equations;

$$\dot{x}_1 = v_1 \tag{1}$$

Then the vehicle dynamics for the first vehicle can be expressed as;

$$\dot{v}_1 = -k_p^1 x_1 + k_p^1 x_2 + k_p^1 d + k_p^1 v_1 + k_p^1 v_2 \tag{2}$$

For the second vehicle

$$\dot{x}_2 = v_2 \tag{3}$$

Vehicle dynamics for the second vehicle can be expressed as

$$\dot{v}_2 = k_p^2 x_1 + k_p^2 x_2 + k_p^2 d + k_p^2 x_3 + k_p^2 x_3 - k_p^2 d + k_d^2 v_1 + 2k_d^2 v_2 + k_d^2 v_3 \quad (4)$$

For the n-1th vehicle

$$\dot{x}_{n-1} = v_{n-1} \quad (5)$$

Vehicle dynamics for the n-1 vehicle can be expressed as

$$\dot{v}_{n-1} = k_p^{n-1} x_{n-2} + k_p^{n-1} x_{n-1} + k_p^{n-1} d + k_p^{n-1} x_3 + k_p^2 x_n - k_p^{n-1} x_{n-1} + k_p^{n-1} d + k_d^{n-1} v_{n-2} - 2k_d^{n-1} v_{n-1} + k_d^{n-1} v_n \quad (6)$$

For the nth vehicle

$$\dot{x}_n = v_n$$

Vehicle dynamics for the n-1 vehicle can be expressed as

$$\dot{v}_{n-1} = k_p^n x_{n-1} + k_p^n x_n + k_p^n d + k_d^n v_{n-1} - k_d^n v_n + u \quad (7)$$

Where

v_i is the velocity of the ith vehicle

x_i is the position of the ith vehicle

k_p^i is the proportional gain

k_d^i is the derivate gain

u is the control unit i.e., the leader.

From the above model equation the value for k_p is constant whereas the value for the k_d is a variable based on the size of the platoon.

1) Leader vehicle: This is conventionally the first vehicle in the platoon. The vehicle is tasked with the roles of establishing and furnishing the platoon with coordinates using the advanced traffic management system [21]. The advanced traffic management system utilized by the platoon leader is vital for the controlling of driving behavior of the other platoon vehicles, the collection of data from the other vehicle and the roadside units, broadcasting of information to the platoon [19]. The movement of the platoon leader forms the reference for all the other platoon vehicles.

2) Member vehicle: These are the vehicles within the platoon that follow the platoon leader and are located neither at the front door at the back [22]. These vehicles receive specified control messages from the leader and the preceding member vehicles.

3) Relay vehicle: This can be any member of the platoon charged with assisting the leader vehicle in conveyance of messages to all the other respective member vehicles.

4) Free vehicle: These are the vehicles that do not belong to any platoon [20]. In the event that they want to join a platoon they will send a request to the leader who will grant permission and that it can perform the join operation.

5) Tail vehicle: This the vehicle located at the tail end of the platoon. it is essential for the inter-platoon communication [19]. The vehicle is vital and responsible for establishment of connection with the next platoon.

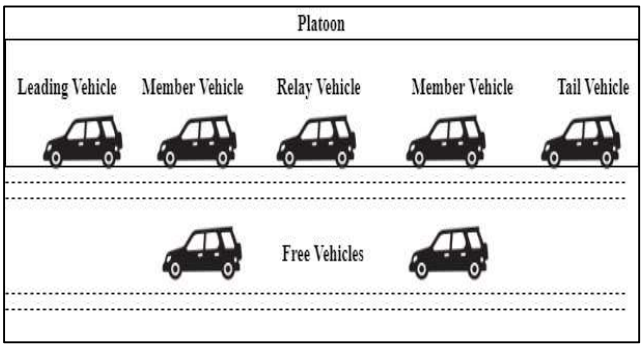

Figure 1 The Model of the platoon

2.2. Communication Model

The intra-vehicle communication is vital in achieving the platoon stability. The stability is maintained by constant and reliable exchange of information between the vehicles in the platoon as illustrated in "Fig. 2". The call mechanism of platoon communication is the V2V scheme. The visible light communication (VLC) system will

be used for the vehicle to vehicle communication in the platoon [23]. The transmission will be such that the flow of the information will be from the leader to the second vehicle to the succeeding vehicle in a consecutive manner. Additionally, there will be no broadcasting the VLC system so that malicious actors can be detected easily. The broadcast mode in this model will be different from the traditional schemes as not all the vehicles in the platoon will be required to transmit an acknowledgement (ACK) to prevent the occurrence of an acknowledgements storm. In case that the transmission fails in broadcast mode, the source vehicle will not retransmit the lost packets. The Request To Send / Clear To Send (RTS/CTS) access mode will not be applied as it will lower performance in the broadcast mode due to the mobility in the platoon and the increased overhead [23]. The longitudinal movement of the vehicles in a Platoon will be affected by the leader therefore the communication framework should ensure that the leader receives information from each vehicle in the platform. Thus, it is assumed that the length of the platform will not exceed the communication range R of the leaders hence restricting the communication range [19]. The vehicle in the platoon will be fixed with a transceiver for communication. In this model, the leader can send information to any member of the platoon while all the other vehicles can only send information to the following member vehicle. The leader will transmit the control information which dictate the behavior of the vehicles such as accident warning, driving behavior and traffic conditions [24]. The non-control information will entail application data such as media, office services and entertainment. The movement of the control information affect the stability and safety of the platoon therefore in this research we will consider the flow of control data.

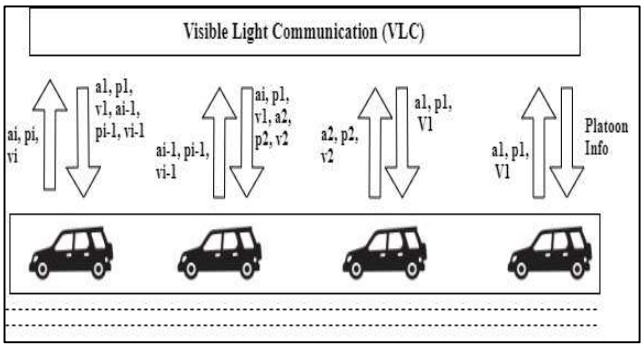

Figure 2 The visible light communication framework for the platoon

2.3. VEHICLE CONTROL MODEL

The dynamics of the platoon vehicle is non-linear but they can be linearized when certain assumptions and feedbacks are applied. Therefore, a simple model is applied for the dynamic model for the longitudinal motion in the platoon. The communication will be based on the leader-predecessor scheme as demonstrated in "Fig. 3". The spacing error can be defined using the following system equations.

$$\epsilon_i = p_{i-1} - p_i - l_{i-1} - \mathcal{g}_{i-des} \quad (6)$$

Where

p_i is the position of the ith vehicle

p_{i-1} is the position of the preceding vehicle

l_{i-1} is the length of the preceding vehicle

$\mathcal{g}_{i-d}$ is the desired gap between the two

At t = 0 at initial condition $\epsilon_i(0)$ is the geared towards the objective of attaining convergence at

$\epsilon_i(t) \rightarrow 0$, where $t \rightarrow \infty$

Taking the initial condition of $\epsilon_i = 0$ the desired position of the ith vehicle can be calculated as

$$p_{i-des} = p_{i-1} - l_{i-1} - \mathcal{g}_{i-des} \quad (7)$$

The desired acceleration can be compute considering the feedback messages such as the speed, acceleration and the position of the preceding vehicle and the position desired by the leader vehicle thus the acceleration will be expressed as;

$$u_{i-des} = (1 - q_1)a_{i-1} + q_1 a_l - q_2(v_i - v_{i-1}) - q_3(v_i - v_l) - q_4 \in_i \quad (8)$$

Where

q_1, q_2, q_3 and q_4 are the design parameters

l denotes the leader

Further, in this model a first-order filter will be utilized to model the signal processing delay and actuator lag in the platoon as demonstrated below.

$$u_{i-des} = (1 + \mu s)u_i \quad (9)$$

Where μ is the collective delay such as actuator delay (which is a constant), sensor detection, processing delays and control delay.

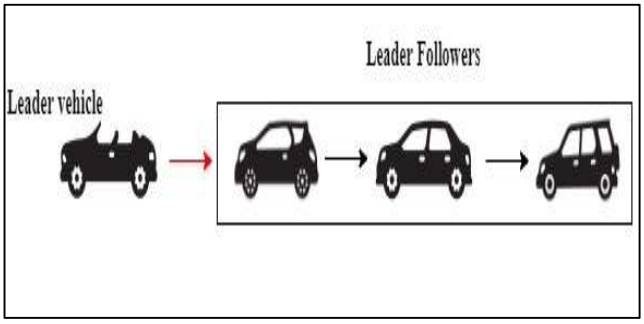

Figure 3 The leader-predecessor flow of information

2.4. Threat Model

In this research we will consider a case of a single actor in control of a vehicle that is in an already established platoon. The vehicle will be travelling at a constant speed as the rest of the members of the platoon and will attempt to destabilize or take control of the platoon [21]. The attacker in this may attain its objective by causing the vehicle under control to subvert or ignore the control information does leading to follower separation. The vehicle under the controller will not obey any laws regarding modification or change in direction of the movement [24]. The attacker's vehicle possesses the same ability as all the vehicles in the platoon. To illustrate that the attacker is capable of destabilizing the platoon operations without possessing nominal control then it will be assumed that the vehicle under control is not the leader of the platoon. The state-pace representation of the linear time-invariant (LTI) system when a vehicle is under the control of an attacker will be represented as

$$\dot{x} = Ax + Bu \tag{12}$$

$$y = Cx \tag{10}$$

Where x is the state of all the vehicles in the platoon and can be expressed as;

$$x = [x_1, v_1, x_2, v_2 \dots, x_n, v_n]^T \in \mathbb{R}^{2n} \tag{14}$$

$A \in \mathbb{R}^{2nx2n}$

$B \in \mathbb{R}^{2nx2}$, has non-zero entries for both the leader and the attacker

C is the identity matrix

$u = [u_l u_a]^T$

u_l is the state of the leader

$u_a = a \sin \omega t$ is the state of the attacker where a is the amplitude of attacker's input and ω is the frequency.

The primary goal of the attacker will be to cause instability in the network through the modifications of the entries of A. The attacker will attain the $a \sin \omega t$ point so as to convey messages and cause instability.

2.5. Priority Scheduling for Attack Detection

This is a non-preemptive algorithm that is commonly used in batch systems. This algorithm will be modified to conform to the commands send by the leader. The control commands from the leader have more precedence that all other commands. All the member vehicles in the platoons will scan for control commands before acting to any other form of instruction. Therefore, during an attack especially Sybil attack the member vehicles will scan for control instructions from the leader. In case of conflicting commands, the vehicle will act on the information with the highest level of precedence. The priority call algorithm will be implemented as demonstrated in "Fig. 4";

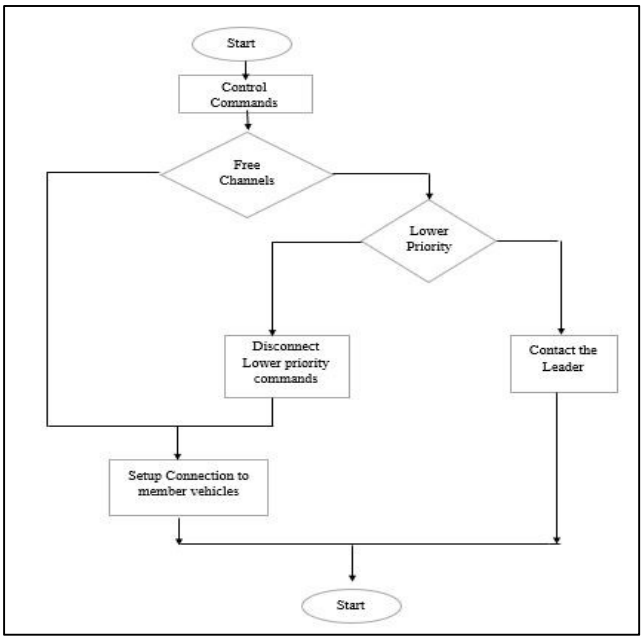

Figure 4 priority call algorithm

3. RESULT

This section talks about the effects, detection and the mitigation of sybil and delay attacks by using priority call algorithm in combination with color-shift keying modulation to protect the platoon alleviating the undesirable impacts such as collisions, oscillations and disintegration in the platoon caused by the attacks.

3.1. Visible Light Communication

The leader is fixed with VLC sensors which uses light to send control communication to the succeeding vehicles in the platoon. The communication from the leader to the second vehicle is dependent on the luminous intensity of the light in the VLC as illustrated in "Fig. 5".

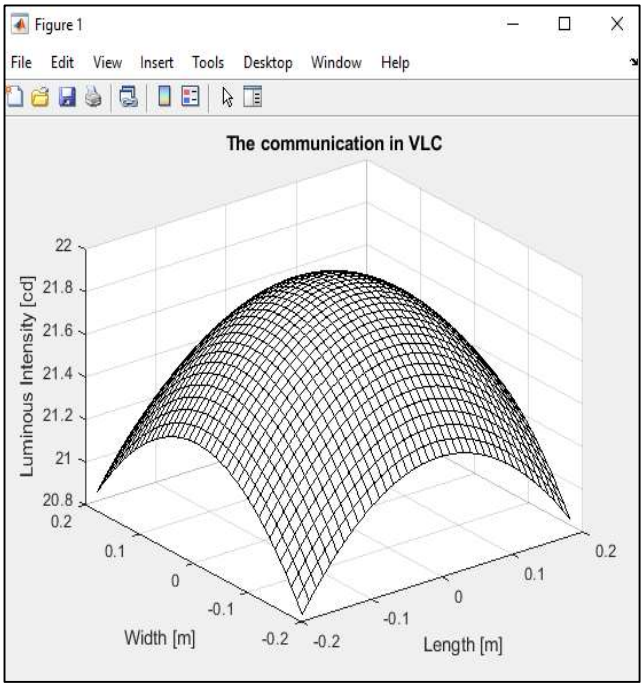

Figure 5 The visible light communication scheme between the platoon vehicles [25]

Thus, using the VLC scheme the normal distribution can be completed as illustrated below for the communication from one vehicle to the next in the platoon.

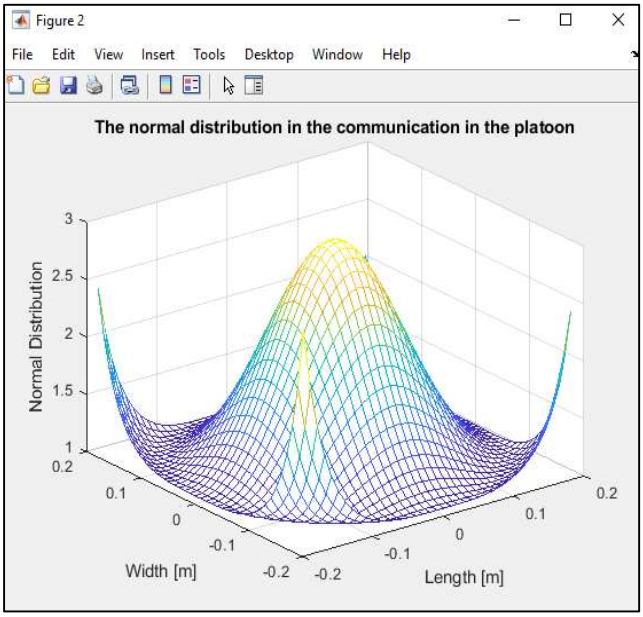

Figure 6 The normal distribution leader and the vehicles in the platoon [25]

Further, the leader uses the flow of communication in the VLC scheme to detect any break in communication caused by a malicious actor. The malicious actor in the platoon will be detected as a break in the light communication between the leader and the rest of the platoon vehicle. The simulation for this proposed framework commenced with the creation of the ideal scenario where the communication of the platoon vehicles via VLC will be greatly impaired by the malicious actor. in "Fig. 6" above illustrate that the connectivity of the vehicles for VLC will increase exponentially with increase in the luminous intensity of the light. The changes in the traffic will not significantly affect VLC communication, therefore, for ideal case we expect the communication between the member vehicles and the leader vehicle to behavior in a similar manner unlike IEEE 802.11p as shown in "Fig. 7", where duration time increase with the increasing of traffic density.

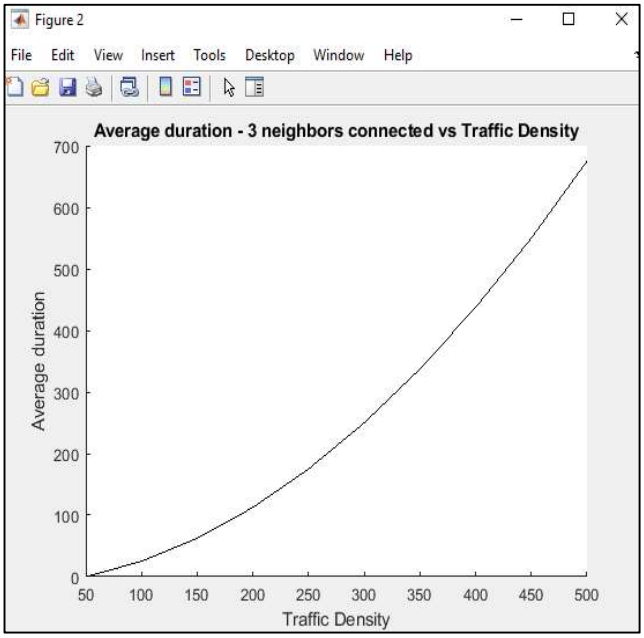

Figure 7 The duration of V2V communication for the normal communication of platoon vehicles. The graph illustrates the time taken for communication between the vehicles in the platoon as the vehicle increases [25]

The average duration describes the delay in the system. The delay behaves in a similar fashion as the VLC communication as rate of communication determine the waiting time for acknowledgement in the system. The average waiting time increases in the system with the increase in the number of vehicles in the traffic as well as the platoon.

3.2 Sybil Attack

The simulation was based on a real scenario where the vehicles in the platoon are expected to negotiate an intersection and take the forward route. In the model the leader will communicate the dynamics of the road to detect the behavior of the vehicles as they negotiate the intersection. The rate of communication of the control information will be based on the VLC communication where the malicious actor will hinder information moving to the vehicle.

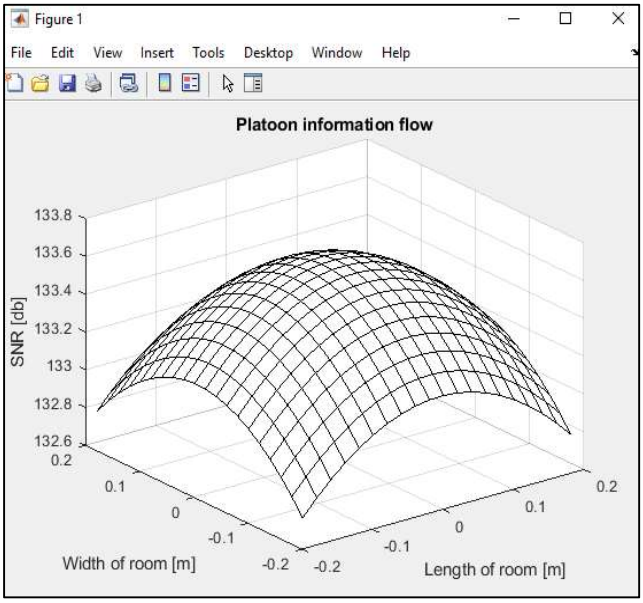

Figure 8 The normal flow of information in the platoon [25]

In the normal scenario the vehicles will communicate the control information between each other through VLC. Alternatively, the attacker will be an impediment to the traditional communication between the vehicles in the platoon. Considering the attacker is located within the platoon vehicles then the VLC scheme integrity will decay rapidly until it become non-existent in cases of longer distances from the leader.

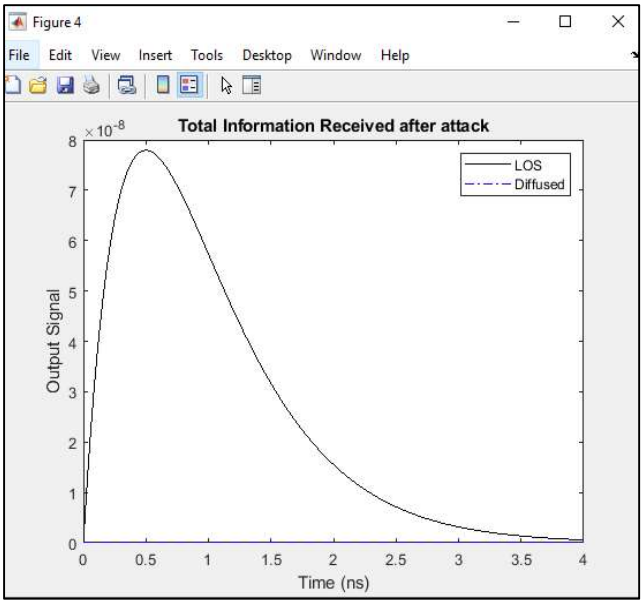

Figure 9 The change in the VLC communication received during the attack in the platoon [25]

The VLC will enable the conveyance of the control information from the leader to the tail vehicle. The proportion of VLC communication should increase to a certain point of integrity where it cannot be affected by the number of vehicles in the platoon provided they are within the range of each platoon member. In the event of an attack the proportion of VLC communication will be compromised thus decrease rapidly hindering the transmission of the control information from the leader to the tail vehicle as illustrated in "Fig. 9". The attack will diminish the efficiency of the diffused VLC hence it will appear nonexistent compared to the LOS.

3.3 Delay Attack

The delay attack will occur in a similar fashion as the Sybil attack in which the attacker will try to take control of the vehicle as well as the follower. "Fig. 10" illustrate the delay leading to the loss of communication in the platoon. The attacker will lead to reduced flow of information via VLC scheme.

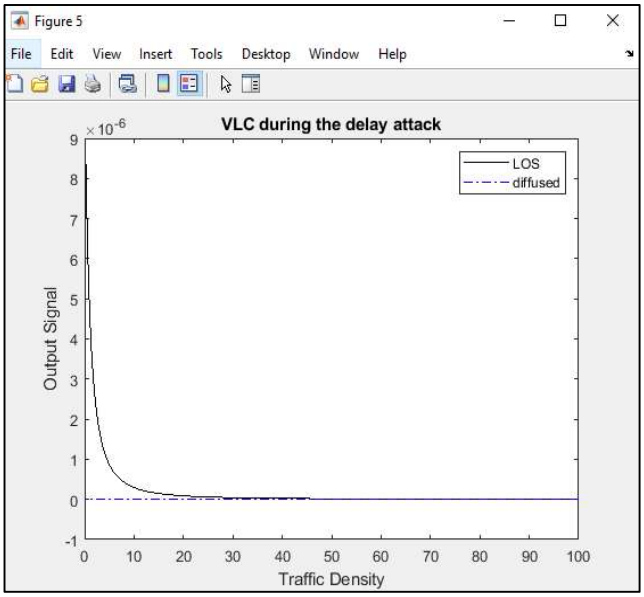

Figure 10 The delay in the communication in the system [25]

3.4 Detection and Mitigation

The second simulation was to detect the attacker where the parameter for the gains and the estimated alterations are identified. The system incorporated a detection and mitigation mechanism. The method was applied to the data used in the attack simulation. "Fig. 11" illustrate that the information flow will build exponentially in the VLC communication as each vehicle waiting for its turn to transmit. Whereas "Fig. 12" illustrate the time taken to detect the attacks with the increase in the traffic density in the platoon.

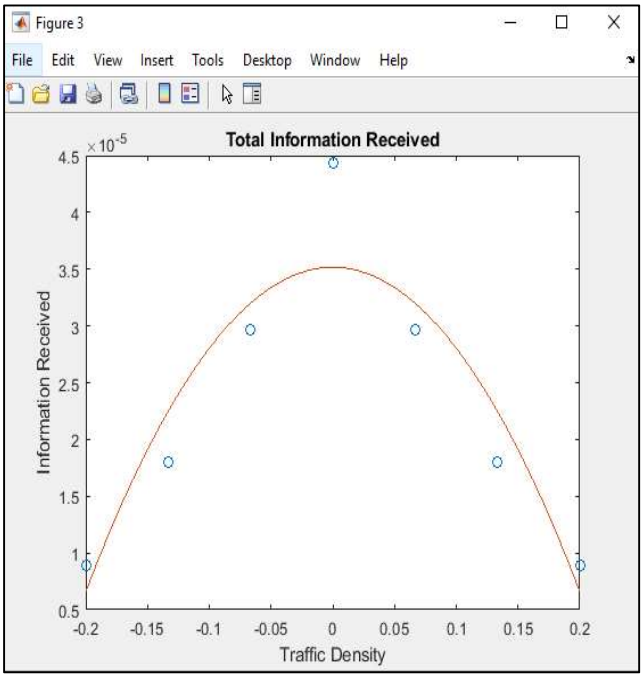

Figure 11 The detection of the attackers and subsequent mitigation. The graph illustrates the communication between the members of the vehicles after mitigation of the attack [25]

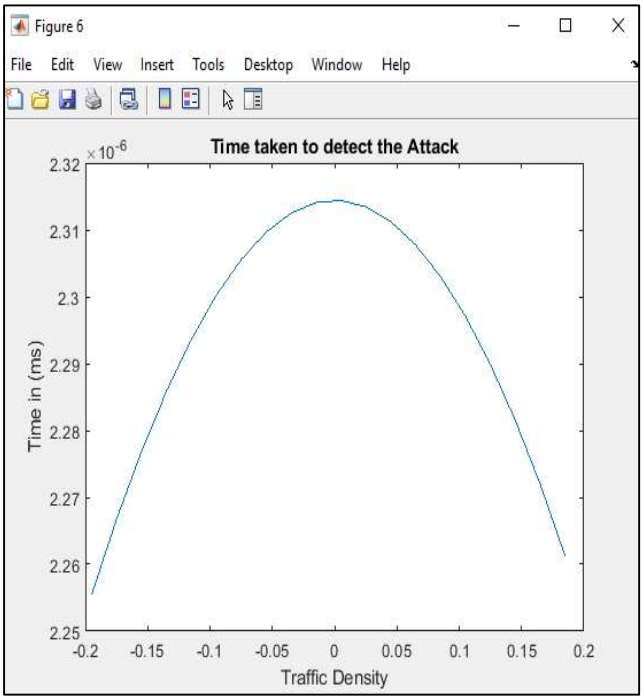

Figure 12 The time taken for the detection of the attacks [25]

To address the attacks, the vehicles should always fetch the control information before acting to other commands. The priority of the control information will prevent splitting at the intersection. For instance, when a vehicle receives a split or turn command which will affect its dynamics such as position and velocity will have to search and check for commands from the leader before acting on the information.

3.5 Color Shift Keying

After detection platoon security will be implemented using the color-shift keying (CSK). CSK is a VLC modulation scheme used to transmit information by altering the light intensity. In this research we recommend a light-to-frequency (LTF) converter. In this system the receiver will decode the symbols with regards to the frequency of transmission. Once there is a drop in the intensity of the light transmitted in the platoon the CSK will be implemented to alter the intensity of the RGB coupling with radio frequency to ensure security of the communication. The CSK will use coded symbols to transmit the control information from the leader.

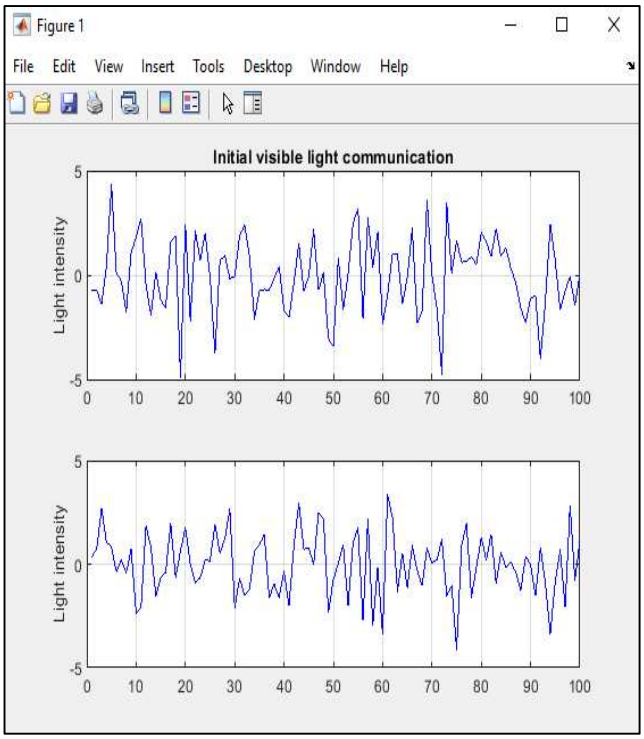

Figure 13 The initial VLC communication after attack [25]

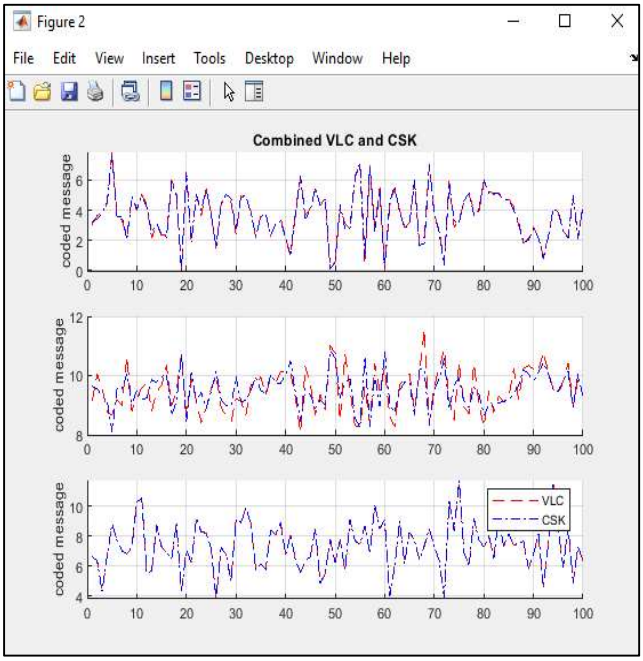

Figure 14 VLC communication coded using CSK [25]

4. CONCLUSION

This research has shown that the vehicular networks have the potential of becoming a vital application of the Ad hoc networks. Platooning is a special application of these networks being applied in autonomous vehicles presenting several security challenges in communication. The security challenges in VANETs and vehicle platoon need to be addressed using new communication perspectives. In vehicle platoon, security consideration is considered as paramount over all other networking elements. The application of a robust security system will ensure the resilience of the vehicle platoon in the presence of interference and other communication problems that can induce an error in VANETs. This research has shown that security for vehicle platoon can be achieved through the application of two techniques to detect and mitigate interruption in the visible light communication algorithm used in the network. The network and the attack scenarios were simulated in MATLAB [25] to create a simplified detection and mitigation system to counter the effects of the breaches and guarantee security thereafter. The results of the research illustrated that a vehicle in the platoon that is under a modified control system and being operated by a malicious actor would interrupt and destabilize the normal operation of the platoon.

The communication of the vehicles in the platoon will provide the first incites on the attacks in the system.

Using MATLAB [25], a model was created to simulate the multiple scenarios of attack. The model created several aspects of the vehicle platoon; the physical operation of the platoon, the communication in the Ad hoc network via visible light communication (VLC), possible security breaches and the effect of attacks on the platoon and the Ad hoc network. The scenarios were created based on the underlying knowledge collected during the literature review. The information gathered led to the decision to incorporate the physical and the network aspect of the vehicle platoon in the simulations. The network design was independent of the vehicles; thus, different communication protocols can be implemented. The defenses were tested using attack scenarios. The behavior of the network was used to identify the different types of attacks. The attacks were mitigated using a variant of the priority call algorithm and the system secured using the color-shift keying algorithm.

Funding

The authors received no financial support for the research, authorship, and/or publication of this paper.

The Declaration of Conflict of Interest / Common Interest

No conflict of interest or common interest has been declared by the authors.

Authors' Contribution

Both authors contributed equally to the design and implementation of the research, to the analysis of the results and to the writing of the manuscript.

The Declaration of Ethics Committee Approval

The authors declare that this document does not require an ethics committee approval or any special permission.

The Declaration of Research and Publication Ethics

The authors of the paper declare that they comply with the scientific, ethical and quotation rules of SAUJS in all processes of the article and that they do not make any falsification on the data collected. In addition, they declare that Sakarya University Journal of Science and its editorial board have no responsibility for any ethical violations that may be encountered, and that this study has not been evaluated in any academic publication environment other than Sakarya University Journal of Science.

REFERENCES

[1] B. Chen, “A cooperative control method for platoon and intelligent vehicles management,” pp. 1–5, 2017.

[2] F. Sakiz and S. Sen, “A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV,” Ad Hoc Networks, vol. 61, pp. 33–50, 2017.

[3] S. Zhao, T. Zhang, N. Wu, H. Ogai, and S. Tateno, “Vehicle to Vehicle Communication and Platooning for EV with Wireless Sensor Network,” pp. 1435–1440, 2015.

[4] S. Rehman, M. A. Khan, T. A. Zia, and L. Zheng, “Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges,” vol. 3, no. 3, pp. 29–38, 2013.

[5] V. L. Hybrid, “IEEE 802.11p and Visible Light Hybrid Communication Based Secure Autonomous Platoon,” IEEE Trans. Veh. Technol., vol. 67, no. 9, pp. 8667–8681, 2018.

[6] S. Ucar, S. C. Ergen, and O. Ozkasap, “Visible light communication in vehicular ad-hoc networks,” in 2016 24th Signal Processing and Communication Application Conference (SIU), 2016, pp. 881–884.

[7] S. Ucar, B. Turan, S. Colen, O. Ozkasap, and M. Ergen, “Dimming Support for Visible Light Communication in Intelligent Transportation and Traffic System,” pp. 1193–1196, 2016.

[8] A. Petrillo, A. Pescap, and S. Santini, “A collaborative control strategy for platoons of autonomous vehicles in the presence of message falsification attacks,” pp. 110–115, 2017.

[9] H. Menouar, “Visible Light Communication,” no. december, pp. 45–53, 2015.

[10] Tseng, Y. Wei, A. Chen, H. Wu, H. Hsu, and H. Tsai, “Characterizing Link Asymmetry in Vehicle-to-Vehicle Visible Light Communications,” pp. 88–95, 2015.

[11] P. Luo, Z. Ghassemlooy, H. Le Minh, and E. Bentley, “Performance analysis of a car-to-car visible light communication system,” no. March, 2015.

[12] M. Y. Abualhoul, M. Marouf, O. Shagdar, and F. Nashashibi, “Platooning Control Using Visible Light Communications : A Feasibility Study,” no. Itsc, pp. 1535–1540, 2013.

[13] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, “A Security Credential Management System for V2V Communications,” pp. 1–8, 2013.

[14] X. U. S. H. S. Hen and U. N. O. F. W. Aterloo, “Complementing Public Key Infrastructure To Secure Vehicular AD HOC Networks Albert Wasef And Rongxing L U , University Of Waterloo,” no. October, pp. 22–28, 2010.

[15] X. Bin, Y. Bo, and G. Chuanshan, “Detection and localization of sybil nodes in VANETs,” DIWANS 2006 - Proc. 2006 Work. Dependability Issues Wirel. Ad Hoc Networks Sens. Networks (part MobiCom 2006), vol. 2006, pp. 1–8, 2006.

[16] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, “Footprint: Detecting Sybil attacks in urban vehicular networks,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 6, pp. 1103–1114, 2012.

[17] M. Stehlik, V. Matyas and A. Stetsko “Towards Better Selective Forwarding And Delay Attacks Detection in Wireless Sensor Networks,” no. April, 2016.

[18] R. S. Sachan, M. Wazid, and R. H. Goudar, “Misdirection Attack in WSN: Topological Analysis and an Algorithm for Delay and Throughput Prediction.” Proceedings of7'h International Conference on Intelligent Systems and Control (ISCO 2013)

[19] Y. Zhang and G. Cao, "V-PADA: Vehicle-Platoon-Aware Data Access in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 5, pp. 2326-2339, 2011.

[20] M. Su. and S. Ahn, "Autonomous platoon formation for VANET-enabled vehicles," in 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, 2016.

[21] H. Hexmoor, S. Alsamaraee and M. Almaghshi, "BlockChain for Improved Platoon Security," International Journal of Information Systems and Computer Sciences, vol. 7, no. 2, pp. 1-6, 2018.

[22] M El-Zaher, B. Dafflon, F. Gechter, and J.-M. Contet, "Vehicle platoon control with multi-configuration ability," Procedia Computer Science, vol. 9, pp. 1503 – 1512, 2012.

[23] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, M. H. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative," IEEE Communications Magazine, vol. 53, no. 6, pp. 126-132, 2015.

[24] J. Liu, D. Ma, A. Weimerskirch and H. Zhu, "Secure and Safe Automated Vehicle Platooning," IEEE Reliability Society, Detroit, 2016.

[25] MATLAB, R2019a (9.6.0.1072779), 64-bit(win 64), March 8, 2019, License Number 968398. Professional License.