Attack Mitigation and Security for Vehicle Platoon

Daniel Kyalo Ndambuki[1,*] and Hitmi Khalifa Alhitmi[2]

[1]*Department of Electrical and Communication Engineering, P.O. Box 3900-30100, Moi University, Kenya*
[2]*Qatar University, P.O. Box: 2713 – Doha, Qatar*
E-mail: danielkyalo116@gmail.com
[*]*Corresponding Author*

Received 18 September 2021; Accepted 27 October 2021;
Publication 07 November 2022

Abstract

This research entails an investigation into enhanced attack detection techniques as a security feature in vehicular platooning. The paper evaluates critical challenges in the security of Vehicular Ad hoc Networks (VANETs) with a focus on vulnerabilities in vehicle platooning. We evaluate the possibilities of securing a platoon through enhanced attack detection following an inside attack while considering current communication-based approaches to vehicular platoon security that have been effective at isolating infected platoon members. This study proposes the use of color-shift keying (CSK) as a security tool for enhanced detection of an apparent platoon attack. We simulate various attack scenarios involving a vehicular platoon communicating via a VLC network and assess the degree of exposure of such networks to three types of attacks – Sybil attacks, delay attacks, and denial-of-service (DoS) attacks. We recommend the use of a light-to-frequency (LTF) converter comprising of a receiver to collect and decode transmitted symbols with regard to the frequency of transmission. Once there is a drop in the intensity of the light transmitted in the platoon, CSK is implemented to alter the intensity

Journal of Cyber Security and Mobility, Vol. 11_4, 497–530.
doi: 10.13052/jcsm2245-1439.1141

of the red, green, and blue (RGB) spectrum coupled with radiofrequency to ensure the security of the communication. CSK will use coded symbols to transmit the control information from the leader using a microcontroller.

Keywords: Vehicle ad-hoc networks (VANETs), vehicle-to-vehicle communication, visible light communication (VLC), vehicular system, network security, color-shift keying (CSK).

1 Introduction

With the evident exponential growth of wireless networks and the Internet, transport systems have evolved tremendously and smartly. Resultantly, vehicular networks have continued to garner more interest among researchers [1]. Vehicular communication occurs both internally (between individual platoon vehicles) and externally (between vehicles and road infrastructure) [2]. The vehicular system has become one of the most important research topics in the development of next-generation traffic safety and management systems. Autonomous vehicles are a rising innovation designed to facilitate efficient transportation and safety. Each year, the lives of over 1.35 million people end in road accidents – between 94% and 96% of these accidents are the result of some type of human error [3, 4]. A proposed remedy to this issue has been to implement an intelligent transportation system (ITS) on automated vehicles for improved safety and maximized efficiency. The National Highway Traffic Safety Administration (NHTSA) categorizes automated vehicles into four levels, ranging between no-automation (level 1) and full automation (level 4). Autonomous vehicles rely on communication systems, such as V2V and vehicle-to-infrastructure (V2I), to wirelessly transmit information between each other. Vehicle-to-everything (V2X), which incorporates V2V, V2I, and other interaction frameworks such as vehicle-to-pedestrian (V2P) and vehicle-to-network (V2N) (see Figure 1), has undergone rapid improvement in recent years [5].

New technologies have emerged as a result of V2X, including blind-spot monitoring, Adaptive Cruise Control (ACC), and parking assistance. V2X is a fast-rising innovation, with approximately 146 million vehicles in the U.S. expected to house the technology by 2029 [6]. The goal of vehicular technology, as considered in this paper, is to facilitate secure V2V and V2I communication and to maintain stability of a vehicular platoon through technologies such as visible light communication (VLC). However, VANETs utilizing VLC as a mode of information transfer among platoon

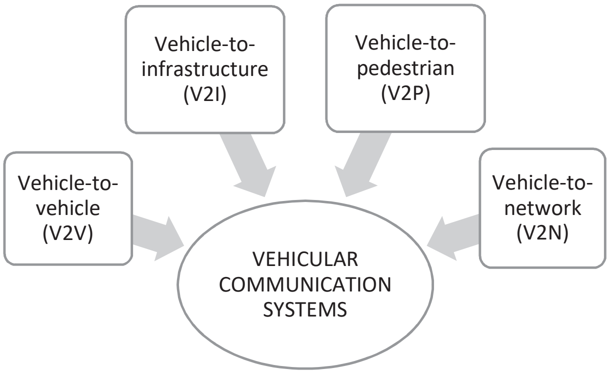

Vehicle-to-infrastructure (V2I)
Vehicle-to-pedestrian (V2P)
Vehicle-to-vehicle (V2V)
Vehicle-to-network (V2N)
VEHICULAR COMMUNICATION SYSTEMS

Figure 1 Vehicular systems communication enabled by V2X technologies has led to increased traffic efficiency, better road safety, and more readily available infotainment services [5].

members remain susceptible to inside attacks which dangerously compromise communication among members and between vehicles and infrastructure.

The goal of this research is to offer a solution towards securing vehicular platoons from malicious inside attacks. Three types of attacks prevalently compromise the stability of a platoon: Sybil attacks and delay attacks which compromise data integrity, and DoS attacks which affect data availability. The three types of attacks primarily compromise V2V and V2I channels thus lending credence to the primary objective of this research of enhancing security through detection in across the two communication channels. In this paper, we approach platoon compromise from a VLC perspective, which has remained pointedly unexplored especially with regard to communication accuracy and faster data transfer speeds. We will simulate various attack scenarios involving a vehicular platoon communicating via a VLC network. We will then demonstrate the effectiveness of color-shift keying (CSK) as an attack detection mechanism for enhanced platoon safety.

The next section will offer background information on wireless information sharing for vehicular systems and the categorization of VANET attacks. Section 3 itemizes the three types of attacks that affect seamless communication in VANETs. Following the occurrence of attacks, Section 4 discusses the message authentication code (MAC) technique for enhanced security by preventing further attacks. Section 5 explains the methodology adopted for the paper, while Section 6 presents results from MATLAB simulations for the detection of the three types of VANET attacks. The paper is concluded in Section 7.

1.1 Contributions and Objectives

This research offers new insights into the use of color-shift keying as a viable solution for the detection of inside attacks within a vehicular platoon. We propose enhanced security at the attack detection stage using the RGB spectrum not as a method of communication between vehicles, but as a way of detecting changes in RGB intensity which then translates to an anomaly. This study also offers fresh insights into VANET vulnerabilities by recreating different network scenarios using a simulation system and assessing the degree of exposure of such networks to these types of attacks.

2 Background

The vehicular system relies on communication technologies that facilitate wireless information sharing – more specifically, V2V communication. In previous work, many technologies have been proposed as possible tools for enhancing communication efficiency in vehicular systems. Common examples include IEEE802.11p, ETSI-G5, and LTE-V2X. Both IEEE802.11p and ETSI-G5 exhibit underperformance issues when their medium access control operations are applied to vehicular networks. Since IEEE802.11p's medium access control utilizes broadcast/clear-to-send as the primary method for safety dissemination, it lacks provisions for addressing issues such as mobility hidden station and asymmetrical radio links (ARL) in V2V communication [8]. ARLs occur when different platoon members attempt to send different messages via the same channel [8]. IEEE802.11p exhibits further issues related to fading and unavailability in its frequency spectrum – these spectrum issues have been addressed in LTE-V2X which offers ultra-high bandwidth, wide coverage, and low latency [9]. However, the inherent lack of sturdy security features in these technologies exposes vehicular networks to malicious attacks which can be significantly averted by using visible light communication (VLC) or millimeter-wave (mm-wave) technology. VLC will ensure higher security due to its directionality properties. A hybrid communication technology, combining VLC and the mm-wave, will exhibit relatively higher security performance when used in a vehicular system. Additionally, a high-speed data rate will facilitate information sharing from different sensors, which include LiDAR for three-dimensional mapping and high-definition video feed for better visuals [2]. In this hybrid communication system, the VLC will be responsible for V2V communication and the mm-wave for V2I. By using visible light to facilitate V2V communication, high-accuracy data, such as speed, acceleration, and position, can be shared between vehicles. Similarly, VLC-enabled V2I will facilitate accurate sharing of data involving road condition and traffic congestion.

2.1 Vehicle to Vehicle Communication

Vehicles start exchanging technical data, such as position, speed, and direction of travel, upon entering a connecting range. The real-time exchange of sensory data (LiDAR or HD video) between vehicles occurs through V2V communication which also features high accuracy for blind-spot and lane-change warning in low visibility conditions. Each platoon consists of the platoon leader and many followers that follow the leader. The platoon leader makes decisions associated with speed, acceleration, deceleration and platoon maneuvers. Due to the multi-access nature of a V2V wireless channel, several factors will lead to delays in the delivery of communication data between members [10]. A limited transmission bandwidth, for instance, implies possible congestion, especially when one radio channel is shared by increasingly many platoon members. Some experiments have even demonstrated that transmission congestion can happen in less-complicated scenarios [11]. Unique challenges ensue in consideration of VANET communication – [10] note that because safety messages must broadcast to the entire platoon, ACK collection from each member must occur, which is practically infeasible and will only further exacerbate the congestion problem. The congestion issue presents a distinct security problem, when taking "security" to mean the quality of being threat-free as defined by measures taken to ensure safety and protection. Many researchers have investigated the state of security in VANETs [11–15] – even so, achieving trustworthiness, which implies several vehicles being able to communicate securely with each other and with road infrastructure, remains a problem. Compromised inter-vehicle communication exposes platoon members to information misuse by attackers. Therefore, guarding communication channels against misuse is important towards preventing accidents and endangerment of people's lives [11].

While there have been scientific efforts to investigate vehicle trustworthiness evaluation capabilities and revocation of suspicious messages, much is still to be addressed in terms of effective detection of untrustworthy data, revocation parameters that accurately predict vehicle behavior, and a response framework that maintains fast and accurate decision making even with an increasing platoon vehicle population. In [13] and [16], the Hybrid Trust Model has been investigated as a solution for trustworthiness of vehicles

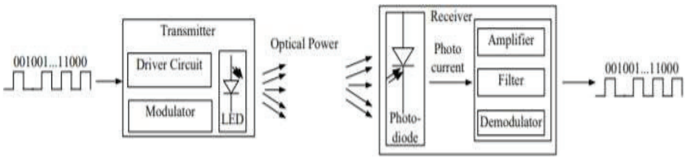


Figure 2 Visible light communication architecture.

in a VANET. [8] and [10] have also investigated the effectiveness of the DSRC/WAVE system in V2V safety communication, and the effect of vehicle influx on communication efficiency. This research will focus attention on V2V and V2I communication and the states of compromise triggered by the three types of malicious attacks.

However, researchers like [17] have scrutinized the VLC approach in scenarios involving limited directionality and lack of access to ample light. VLC systems use visible light in the 380 nm to 750 nm wavelength range. The VLC receiver will only receive signals located in the same room as the transmitter in the arrangement illustrated in Figure 2. The quality of data reception in such cases appears to reduce significantly. Restricted light coverage makes it difficult to intercept data from the outside and thus limits the availability of data to attackers while still allowing communication between vehicles [17]. Further, despite the advanced nature of VLC technology, malicious actors can still compromise the stability of the platoon by listening or hacking into channel communication lines. Addressing communication vulnerabilities will require the use of a secret key in asymmetric cryptography. The sender and receiver agree on a secret key generated using a key establishment protocol. A public key infrastructure (PKI) will generate public-private key pairs which allow the communicating entities to produce digital signatures that encrypt and decrypt data sent over the network (see Figure 3) [18].

Public Key Infrastructure (PKI) is a framework where service integration is related to cryptography. PKI provides access control, integrity, confidentiality and authentication. To enable both users and computer to exchange data securely over the network, PKI supports the distribution of the public key. The components of PKI include software, hardware, policies and standards to manage revocation of keys, distribution, administration, and digital certification. Four issues must be addressed before data transmission can occur:

1. Ensuring the confidentiality of the message.
2. Ensuring that during the transmission, the message does not undergo any modifications.

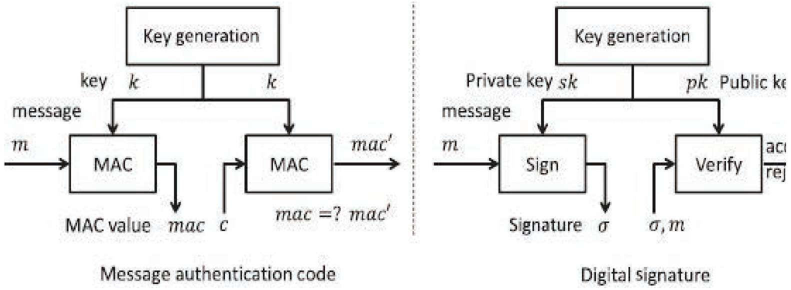


Figure 3 Message authentication code and digital signature assignment in sender/receiver interactions [19].

3. Since the sender and receiver do not know each other, the sender must provide proof of authenticity of the sent document.
4. Ensuring that the receiver gets the message and does not reject it in future.

2.2 VANET Attacks

At present, several types of attacks pose a significant threat to any kind of network, and especially wireless networks. VANET systems need a lot of security services to protect the messages sent and the data exchanged from the leader to the followers and vice versa. The various security requirements include:

- Availability: An essential security point in modern vehicular systems is uninterrupted communication availability between the commander and the rest of the platoon. The attacker may choose to penetrate the network from several different attacking points which may disable the server from relaying sender-receiver messages.
- Confidentiality: It is important to maintain data confidentiality in message details sent between the commander and the platoon.
- Integrity: This is the most critical security point because lost integrity results in costly damage. Data integrity refers to security controls that readily detect any substitutions or modifications made to the data through unauthorized access [20]. Here the recipients should make sure that the messages are correct and from the valid source.

In order to achieve the goal, a secure network must first identify the types of attackers and their ability and the nature of what they do attacks to disrupt

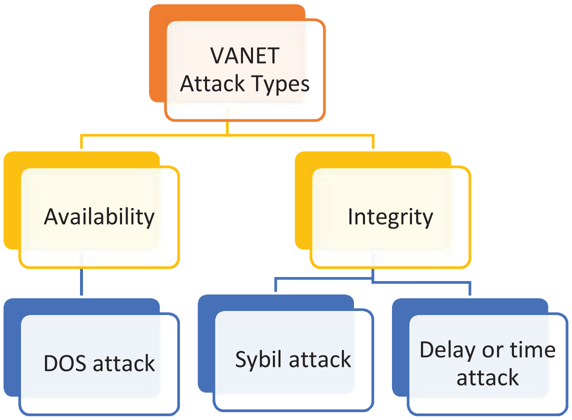


Figure 4 The various types of attacks in VANET.

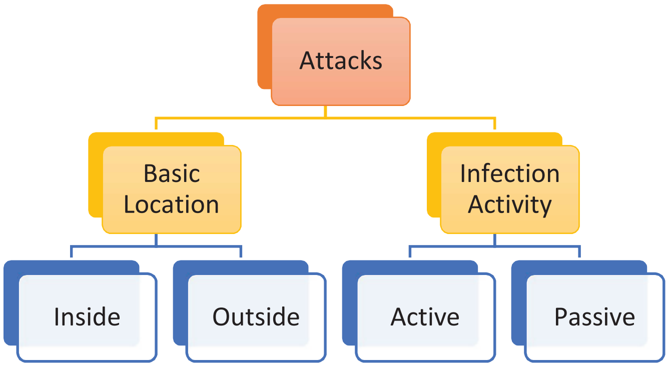


Figure 5 Categories of attacks in VANET.

the network and penetration. Attackers are therefore classified into two main categories as illustrated in Figure 5.

- First, we can classify attackers in terms of activity (an active attacker or a passive attacker). An active attacker can disrupt a communication network or block messages. A passive attacker intercepts network channels or steals data without destroying it; as such, passive attacks do not cause inconveniences or harm but result in unauthorized monitoring of data activity.
- Second, we can classify the attackers in terms of attack direction either as being inside or outside the attacking squad. The internal striker is considered more dangerous than the outside because they retain more

details about the squad. Moreover, identifying an internal attacker is more complicated.

3 Types of Attacks

The goal of this research is to secure vehicular platoons from malicious inside attacks. Three types of attacks prevalently compromise the stability of a platoon: Sybil attacks and delay attacks which compromise data integrity, and DoS attacks which affect data availability as shown in Figure 4.

3.1 Sybil Attack

Sybil attacks are catastrophic for VANETs. In a Sybil attack scenario, a vehicle, which also acts as a node, behaves as if it has multiple identities. The attacker compromises the communication network by generating many fake identities meant to disrupt network protocols. The attack disables network nodes from identifying the actual source of information in the network. Attackers achieve success by shaping networks to function in a particular way. For instance, the attacker can change the vehicles' scheduled route. In addition to being a dangerous form of attack, a Sybil attack is quite sophisticated, which makes it one of the most difficult attacks to detect [21]. It becomes riskier on networks that employ geographical routing as the attacker creates confusion by claiming that the vehicle is in several positions by sending incorrect information on the actual vehicle position. Besides, it could show events occurring in positions that differ from the anticipated position. Node Impersonation Attack is a common type of Sybil attack. In VANETs, each vehicle has a unique identifier, just like IP addresses of devices in a network, and the vehicles use this unique ID to communicate with each other [21]. However, if there is a sudden change in the vehicle ID without the knowledge of the RSU or the network, a Sybil attack may occur as the changed ID is re-introduced as a different vehicle. Each RSU will have unique identification and an associated certificate for a digital signature [22]. Therefore, a compromised vehicle involved in a traffic accident may change its current ID to appear as if it was still moving. Consequently, other vehicles in the network view this vehicle as not being among the vehicles involved in the accident – these cars will collectively be considered affected by the attack even though the Sybil attack only targeted one car (see Figure 6). The malicious vehicle could be used to execute attacker goals by sending incorrect information about the road conditions to the surrounding RSUs.

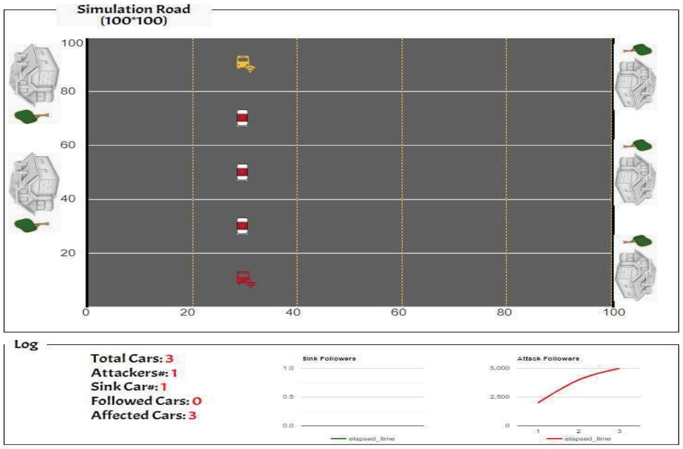
3.2 DoS Attack

Denial-of-Service (DoS) attacks are designed to ensure that system services are unavailable. This usually occurs in cases where the attacker sends too many requests that exceed the system capabilities. In VANETs, the aim of the DoS is to shut down the network established by RSUs and to halt communication between vehicles and RSUs [21]. As a result of a DoS attack, vehicles cannot communicate with each other, and technical information, such as road status, is unavailable, resulting in severe consequences. Therefore, for one affected car in a three-member platoon, information on the other two cars becomes unavailable (see Figure 7).

A Distributed Denial-of-Service (DDoS) attack entails launching an attack from different node locations, thereby complicating the detection process. Nodes launching a DDoS attack could target both the vehicles and the RSUs comprising the road infrastructure. In this research, we will aim to secure the platoon from DOS attacks since the attacker only has one access point and therefore cannot perform a DDoS attack.

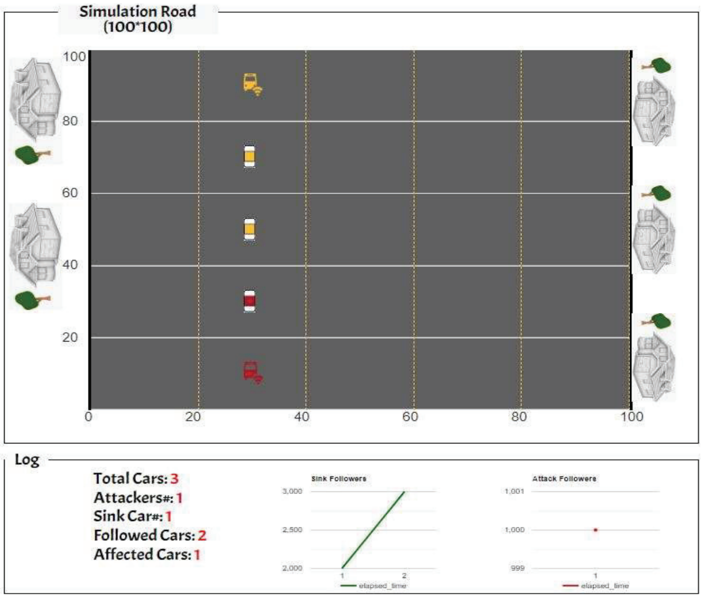
3.3 Delay Attack

This type of attack is one of the eminent types that can cause extensive damage, especially considering the need to sustain high data rates, total dependence, and time accuracy. This type of attack involves adding extra time to each message sent hence causing a delayed output which compromises



Total Cars: 3
Attackers#: 1
Sink Car#: 1
Followed Cars: 0
Affected Cars: 3

Figure 6 Sybil attack.



Total Cars: 3
Attackers#: 1
Sink Car#: 1
Followed Cars: 2
Affected Cars: 1

Figure 7 DOS attack.

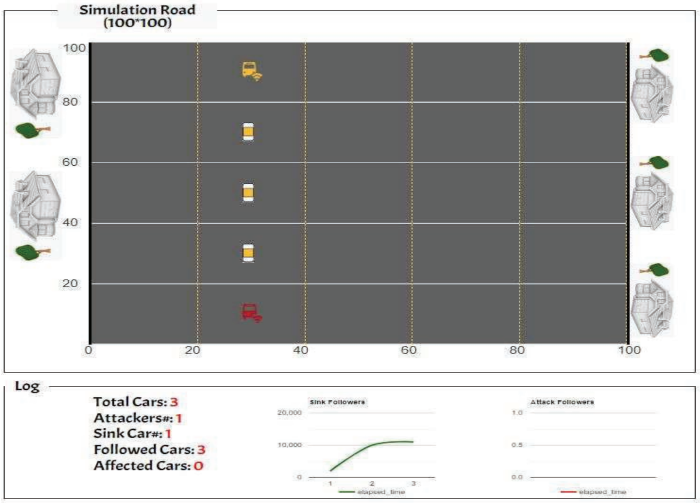
network functionality. Attackers do not alter or fabricate the contents of the message but only create a delay in the message time slot [7]. Therefore, the delay attack delays communication between vehicles in a platoon – because no direct effect impacts any vehicle, platoon movement proceeds normally but jeopardizes efficiency across the entire platoon (see Figure 8).

4 Outside Attacks Security Techniques

4.1 Message Authentication Technique

The message authentication code (MAC) protects the integrity and validity of a message by generating a value (authentication tag) which validates that the message has not been altered [23]. The MAC method consists of several processes as presented in Figure 9:

- First, it is necessary to determine the authentication code from the sender by inserting the message into a complex mathematical process to extract the code to prove the character of the sender.
- Next, the sender in the network adds the code from the first step to the message without encryption, and then sends it to the platoon vehicles.



Total Cars: 3
Attackers#: 1
Sink Car#: 1
Followed Cars: 3
Affected Cars: 0

Figure 8 Delay attack.

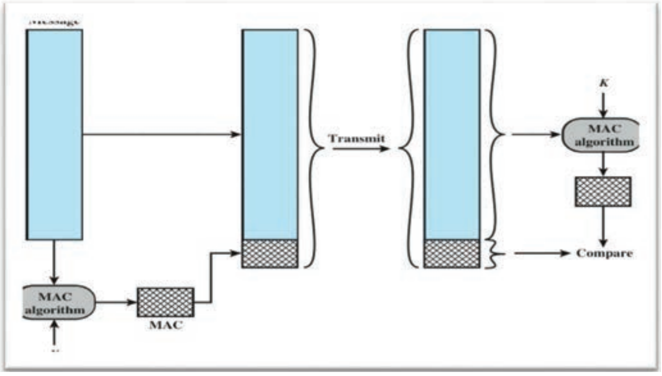


Figure 9 MAC technique.

- Thirdly, upon reception by a vehicle in the platoon, the message and the code are processed separately. The message is then injected into the same intricate process used by the sender and then the unique code is extracted in the car.
- Finally, the platoon member compares the code accompanying the message with the new code generated at the receiving end. If a similar code is realized, the message is delivered to the target sender. But if they are not equal, this message is flagged as inauthentic.

5 Methodology

This section will evaluate the three internal integrity attacks, that is, Sybil attack, DoS Attack, and delay attack. The three attacks have been evaluated in the previous section, and they tend to affect VANETs, especially in the platooning of vehicles. The proposed VLC design will improve the structure and communication of the platoon, and a simulation design will be used to understand the nature of attacks and of the proposed solution.

5.1 The Platoon Model

The structure of the platoon will be based on spatial positions and functionalities in which case each vehicle is classified into several roles as illustrated in Figure 10. The behavior of each vehicle in the platoon based on this model will rely not only on the driver's objectives, but also on the control and management processes performed by the platoon leader [24]. Vehicles transmit request messages in case a driver might need to alter the driving behavior to match up with individual needs such as the need to rest or arrival at the destination. This characteristic will be vital in case of attacks, especially internal breaches [25]. Upon reception of the request, the leader will make a judgement based on the condition of the traffic at the time of the 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 fleet stability. 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 equation:

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

The vehicular dynamics for the first vehicle can be expressed as:

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

For the second vehicle,

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

And the dynamic equation for the second vehicle can be expressed as:

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

$$\vdots$$

For the n-1$^{\mathrm{th}}$ vehicle,

$$\dot{x}_{n-1} = v_{n-1}$$

And the corresponding dynamic equation for the n $-$ 1 vehicle can be expressed as:

$$\begin{aligned}\dot{v}_{n-1} = k_p^{n-1}x_{n-2} + \ & k_p^{n-1}x_{n-1} + k_p^{n-1}d \\ & + k_p^{n-1}x_3 + k_p^2 x_n - k_p^{n-1}x_{n-1} + k_p^{n-1}d + k_d^{n-1}v_{n-2} \\ & - 2k_d^{n-1}v_{n-1} + k_d^{n-1}v_n\end{aligned}$$

For the n$^{\mathrm{th}}$ vehicle,

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

Vehicle dynamics for the n$^{\mathrm{th}}$ vehicle can be expressed as:

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

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 k_d is a variable based on the size of the platoon.

5.1.1 Leader vehicle

This is conventionally the first vehicle in the platoon. The vehicle is tasked with the role of establishing and providing the platoon with coordinates using the advanced traffic management system [26]. The advanced traffic management system utilized by the platoon leader is vital for controlling the driving behavior of other platoon vehicles, the collection of data from other vehicles and the roadside units, and broadcasting information to the platoon [24]. The movement of the platoon leader forms the reference frame for all other platoon vehicles.

5.1.2 Member vehicle

These are the vehicles within the platoon that follow the platoon leader and travel either ahead of or behind the leader [27]. These vehicles receive

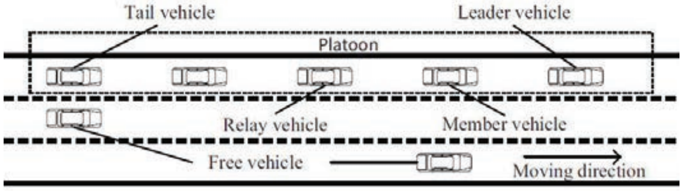


Figure 10 The model of the platoon.

specified control messages from the leader and the preceding member vehicles.

5.1.3 Relay vehicle

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

5.1.4 Free vehicle

These are the vehicles that do not belong to any platoon [25]. 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.

5.1.5 Tail vehicle

This is the vehicle located at the tail end of the platoon. It is essential for inter-platoon communication [24]. The vehicle is vital and responsible for the establishment of a connection with the next platoon.

5.2 Communication Model

Intra-vehicle communication is vital towards achieving platoon stability. The stability is maintained by a constant and reliable exchange of information between vehicles in the platform, as illustrated in Figure 11. The principal mechanism for platoon communication is the V2V scheme. The VLC system will be used for vehicle-to-vehicle communication within the platoon [28]. 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

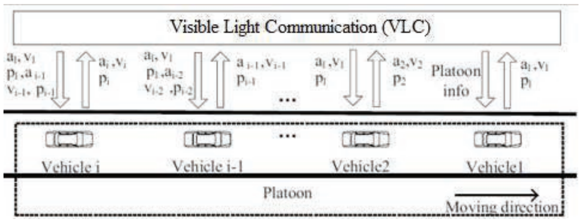


Figure 11 The visible light communication framework for the platoon.

prevent the occurrence of an acknowledgements storm. In the event of a failed transmission in the broadcast mode, the source vehicle would not retransmit lost packets. The RTS/CTS access mode will not be applied as it will lower performance in broadcast mode due to mobility in the platoon and increased overhead [28].

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 [24]. 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 dictates the behavior of the vehicles, such as accident warning, driving behavior, and traffic conditions [29]. The non-control information will entail application data, which includes media, office services, and entertainment. The transfer of control information affects platoon stability and safety; therefore, in this research, we will consider the flow of control data.

5.3 The 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 Figure 12. The spacing error can be defined using the following system equations.

$$\epsilon_i = p_{i-1} - p_i - l_{i-1} - g_{i-des}$$

Figure 12 The leader-predecessor flow of information.

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
g_{i-des} 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

$$\epsilon_i(t) \to 0, \quad \text{where } t \to \infty$$

Taking the initial condition of $\epsilon_i = 0$ the desired position of the i$^{\text{th}}$ vehicle can be calculated as

$$p_{i-des} = p_{i-1} - l_{i-1} - g_{i-des}$$

The desired acceleration can be computed by considering the feedback data such as speed, acceleration, position of the preceding vehicle, and the position desired by the leader vehicle. Therefore, acceleration will be expressed as:

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

Where the variables q_1, q_2, q_3 and q_4 represent the design parameters and l denotes the leader.

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

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

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

5.4 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 [26]. The attacker in this scenario may achieve the intended objective by causing the vehicle under control to subvert or ignore the control information thus leading to follower separation. The vehicle under attacker control will not obey any laws regarding modification or change in the direction of the movement [29]. 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 attacker control is not the leader of the platoon. The state-space representation of the linear time-invariant (LTI) system when a vehicle is under the control of an attacker will be represented as

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

$$y = Cx$$

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

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

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

$$B \in \mathbb{R}^{2nx2},$$

and 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 the attacker's input, and ω is the frequency.

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

5.5 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 sent by the leader. The control commands from the leader have more precedence than

Algorithm 1 Finding the attacker gain to make the platoon string unstable

```
Input: $k_d, n$ and $\omega$ (a normal vehicle gain, platoon size, and frequency)
Output: $\widetilde{k}_d$ (gain for the attacker which makes the platoon string unstable)
    $i \leftarrow$ first transfer function affected by the attacker;
    $\propto (\widetilde{k}_d)^2 + \beta(\widetilde{k}_d) + \gamma > 0 \leftarrow \Im(G_i)^2 + \Re(G_i)^2 > 1$;
    $\Delta \leftarrow \beta^2 - 4 \propto \gamma$;
    if $\alpha > 0$ and $\Delta > 0$ then
        $\widetilde{k}_d$ should be chosen between $\frac{-\beta \mp \sqrt{\Delta}}{2\alpha}$
    else if $\alpha < 0$ and $\Delta > 0$ then
        $\widetilde{k}_d$ should be chosen out of $\frac{-\beta \mp \sqrt{\Delta}}{2\alpha}$;
    else if $\alpha < 0$ and $\Delta < 0$ then
        an attacker cannot make the platoon string unstable;
    else if $\propto = 0$ then
        $\widetilde{k}_d < \frac{-\gamma}{\beta}$;
    else
    end if
```

all other commands. All the member vehicles in the platoons will scan for control commands before responding to any other form of instruction. Therefore, during an attack, especially a Sybil attack, the member vehicles will scan for control instructions from the leader. In the case of conflicting commands, the vehicle will act on the information with the highest level of precedence. The priority call algorithm is implemented as demonstrated in Figure 13.

6 Results

6.1 Visible Light Communication

The leader is fixed with VLC sensors which use 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 the graphical scheme in Figure 14.

Thus, using the VLC scheme, the normal distribution can be completed as illustrated in Figure 15 for the communication from one vehicle to the next in the platoon.

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 the proposed framework commenced with the creation of an

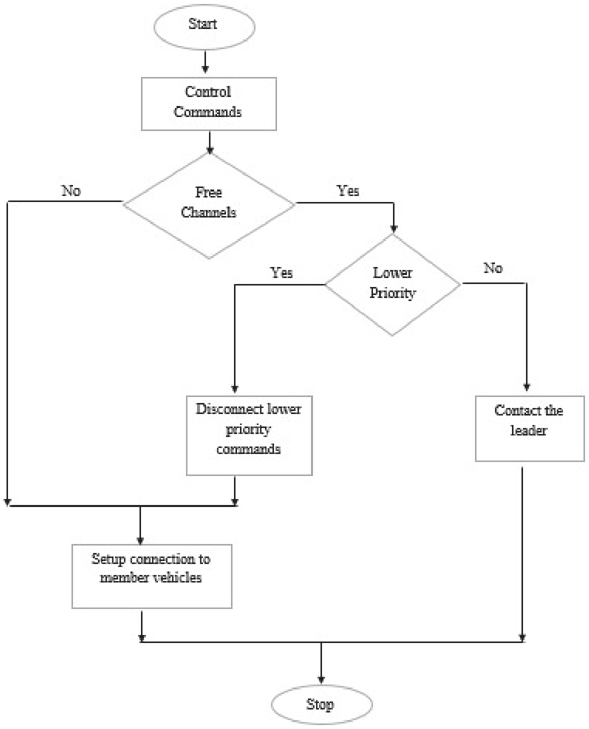


Figure 13 Priority call algorithm to allow vulnerable platoon vehicle act on the information with the highest level of precedence.

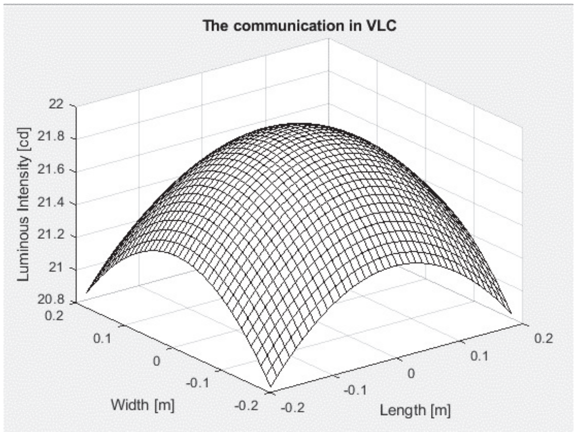


Figure 14 The visible light communication scheme between the platoon vehicles.

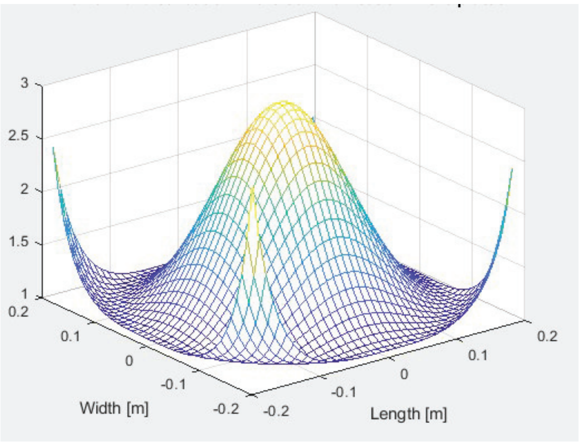


Figure 15 Normally distributed average-value vehicle speeds against connectivity in the free-flow state of traffic. The bell curve implies efficient leader-vehicle communication.

ideal scenario where the communication of the platoon vehicles via VLC was greatly impaired by the malicious actor. Figure 14 illustrates how the connectivity of the vehicles for VLC increases exponentially with an increase in luminous intensity of the light (see Figure 16). Changes in the traffic do not significantly affect VLC communication and, therefore, for an ideal case, we expect the communication between the member vehicle and the leader vehicle to behave in a similar manner. As illustrated in Figure 16, the time delay in V2V interaction expectedly increases as the number of vehicles in the platoon increases.

The average duration describes the delay in the system. The delay acts in a similar manner as the VLC communication whereby the rate of communication determines the waiting time for acknowledgement in the system [30]. The average waiting time increases in the system with an increasing number of vehicles in the traffic as well as in the platoon.

6.1.1 DoS attack

The evaluation of the proposed DoS attack in the system was modelled using jamming nodes. The nodes simulated the communication between the vehicles in the platoon using the VLC scheme [2]. In this scenario, we simulated the behavior of the normal platoon and the platoon under DoS attack, that is, the greedy attack. The back-off parameters in the system were manipulated to allow for reliable communication between the DoS

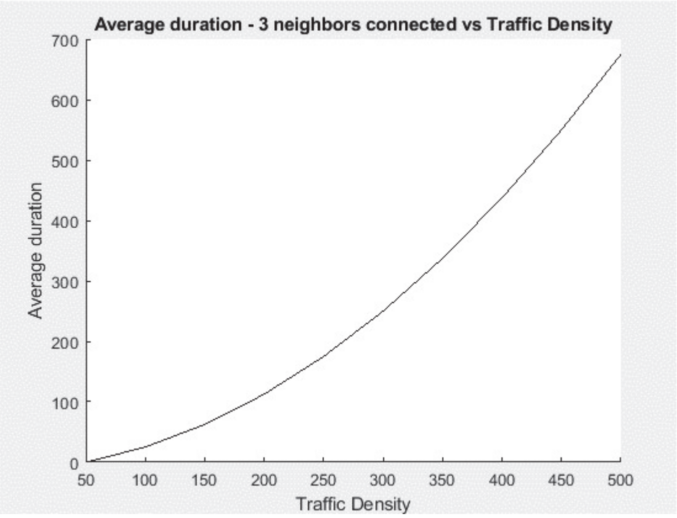


Figure 16 The duration of V2V communication for the normal communication of platoon vehicles. The graph illustrates the time taken for communication between platoon vehicles as the vehicle count increases from two to three vehicles.

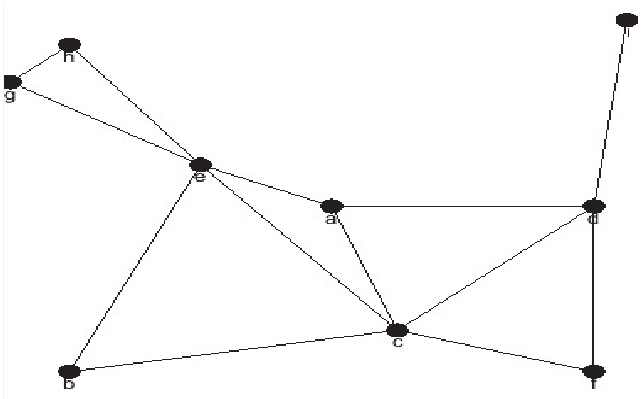


Figure 17 Possible locations of jammers for DoS attacks. This simulation presents the initial configuration of the DoS attackers in the platoon.

nodes (see Figure 19) [26]. The legitimate nodes made up the majority of the system; therefore, computation of the ACK and the data rate was easy. Figure 18 illustrates the different nodes, with the central nodes a, e and c being the attack nodes.

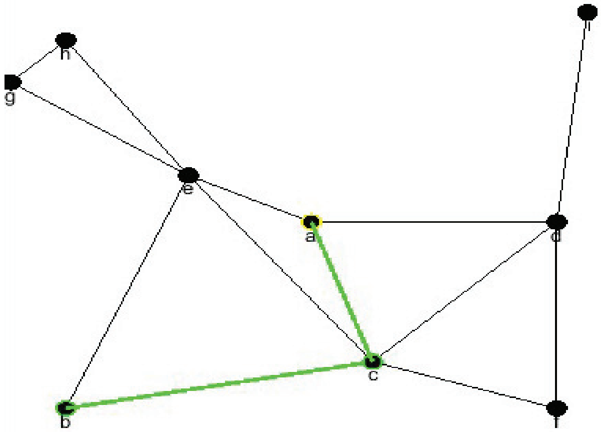
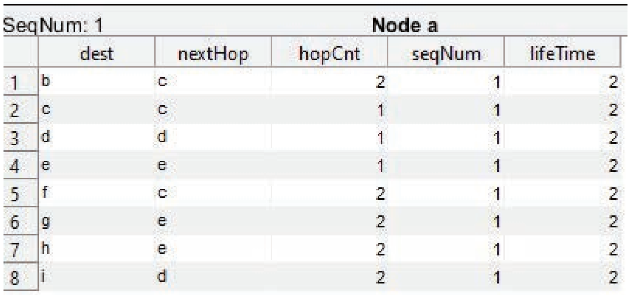


Figure 18 Communication between nodes *a* and *b* through node *c*. connectivity between the nodes represents the interaction of vehicles in the platoon.



SeqNum: 1 **Node a**

	dest	nextHop	hopCnt	seqNum	lifeTime
1	b	c	2	1	2
2	c	c	1	1	2
3	d	d	1	1	2
4	e	e	1	1	2
5	f	c	2	1	2
6	g	e	2	1	2
7	h	e	2	1	2
8	i	d	2	1	2

Figure 19 The parameters of transmitting from node a to other nodes.

6.1.2 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 as in Figure 20 above. In the model, the leader will communicate the dynamics of the road to detect the behavior of the vehicles as they negotiate the intersection [31]. The rate of transfer of the control information will be based on VLC where the malicious actor will hinder information moving between vehicles.

In a normal scenario, the vehicles will communicate the control information between each other through VLC taking the form in Figure 21. Alternatively, the attacker will be an impediment to the traditional communication between the vehicles in the platoon. Considering the attacker is located

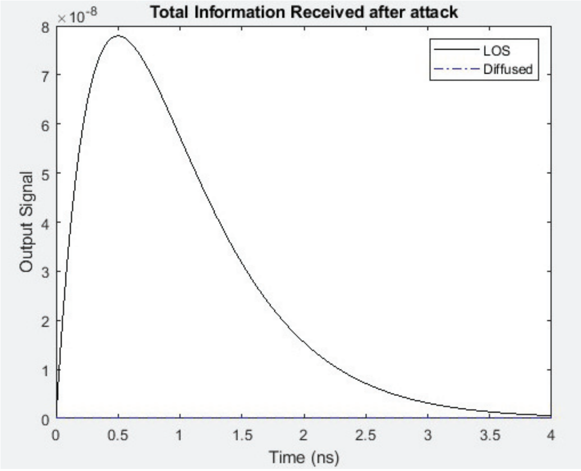


Figure 20 The visible-light view of an intersection. This visible-light image illustrates the view of the malicious actor at an intersection. The actor operating independently has three options rather than waiting for the command from the platoon leader.

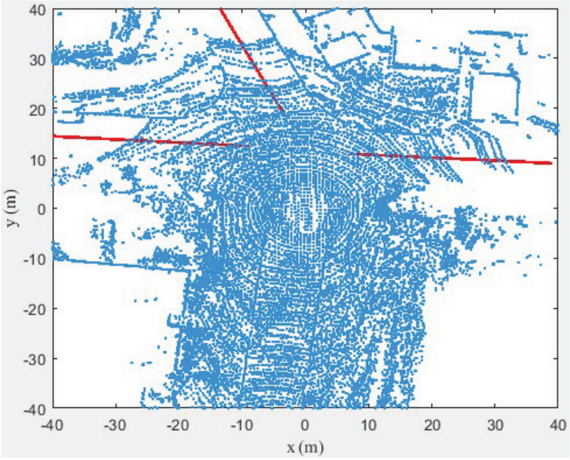


Figure 21 The normal flow of information in the platoon.

within the platoon vehicles, then the VLC scheme integrity will decay rapidly until it becomes non-existent in cases of long distances from the leader [28].

VLC will enable conveyance of control information from the leader to the tail vehicle. The proportion of VLC should increase to a certain point of integrity beyond which it cannot be affected by the number of vehicles in

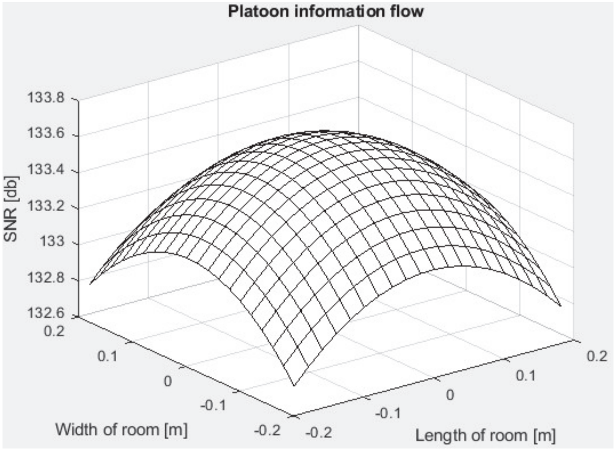


Figure 22 The change in the VLC communication received during the attack in the platoon.

the platoon provided they are within the range of each platoon member [32]. In the event of an attack, the proportion of VLC becomes compromised and thus decreases rapidly which hinders the transmission of control information from the leader to the tail vehicle as illustrated in Figure 22. The attack will diminish the efficiency of the diffused VLC and will hence be non-existent compared to the Line-of-Sight (LOS).

6.1.3 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 the follower [31]. Figure 23 illustrates the delay leading to the loss of communication in the platoon. The attacker will lead to reduced flow of information via VLC scheme.

6.2 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 [24]. Figure 24 illustrates how information flow will build exponentially in the VLC communication as each vehicle waits for its turn to transmit. Correspondingly, Figure 25 illustrates the time taken to detect attacks with increase in traffic density in the platoon. Figure 26

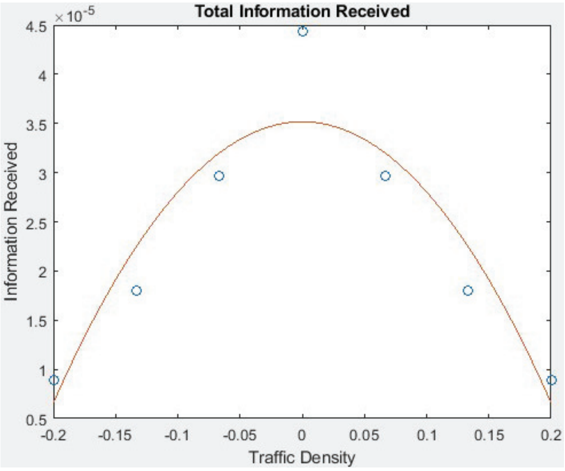


Figure 23 The delay in communication in the system.

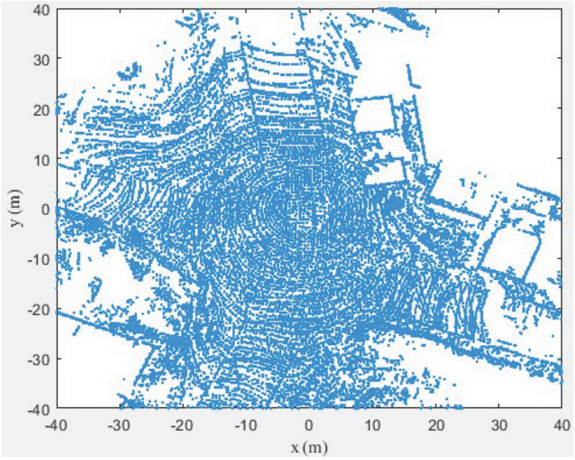


Figure 24 The detection of the attackers and subsequent mitigation. The graph illustrates the communication between the members of the vehicles after mitigation of the attack.

illustrates how the intersection should appear when all the vehicles in the platoon wait for leader communication. The leader will provide information for the position and the velocity of the vehicle in the platoon.

To address the attacks, the vehicles should always fetch control information before responding to other commands – this is illustrated in Figure 27. 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

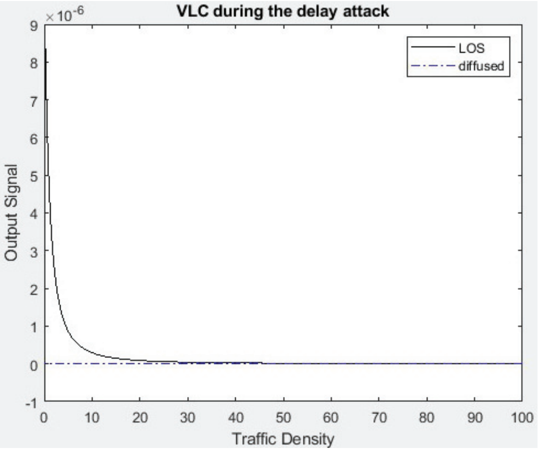


Figure 25 The time taken for the detection of the attacks.

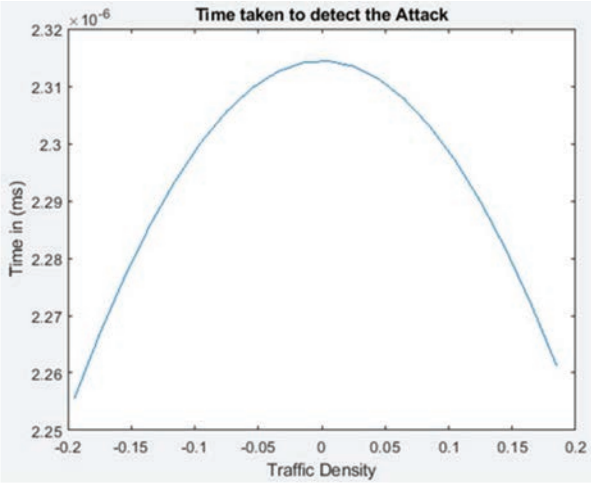


Figure 26 The normal view of the intersection from member vehicle awaiting leader control information. This is the ideal view where the members of the platoon are expected to await control commands from the leader.

affect its dynamics, including its position and velocity, it will have to search and check for commands from the leader before acting on the information.

The proposed security solution for the platoon following the attack uses color-shift keying (CSK). CSK is a VLC modulation scheme used to transmit information by altering light intensity. In this research, we recommend a

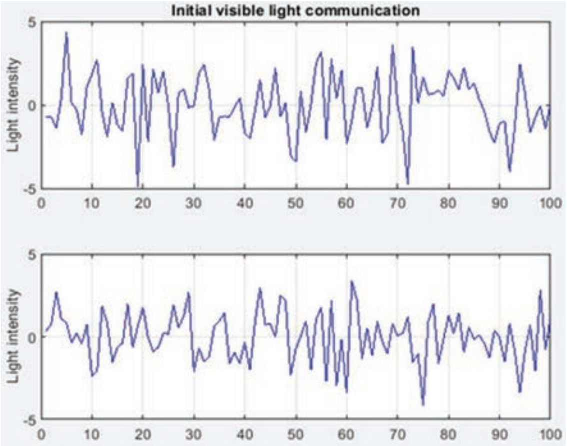


Figure 27 The initial VLC communication after attack.

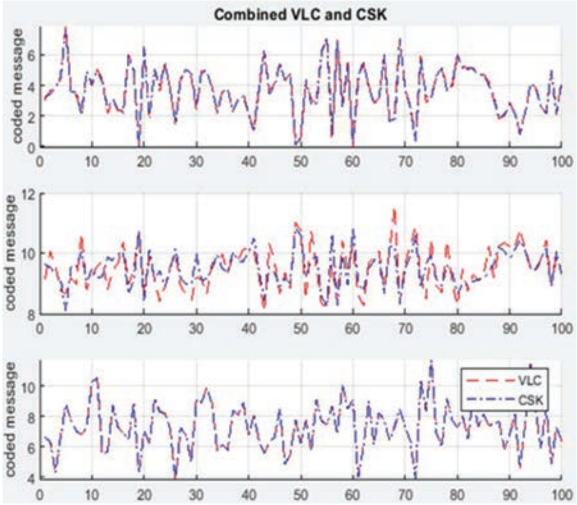


Figure 28 VLC communication coded using CSK.

light-to-frequency (LTF) converter. The receiver will decode the symbols in line with 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 coupled with radiofrequency which will guarantee communication security – the communication outlay for CSK is illustrated in Figure 28. The CSK will use coded symbols to transmit the control information from the leader using a microcontroller.

7 Conclusion

This research paper evaluated the key challenges in the security of VANETs with a focus on the vulnerabilities of the vehicle platooning. The VANET in this research uses priority calls for communication with each priority call being non-preemptive (it will wait for the schedule communication to terminate or go into waiting state). To this end, the algorithm coupled with the VLC will constantly scan the communication against the predestined priority information. The control information relayed from the leader to the second vehicle and to the third vehicle has the highest precedence in the communication channel. Any occurrence of a violation in the communication priority order within the vehicular interaction hierarchy will trigger a security flag that will be detected by the control center in the leader vehicle. The flagging will then incite corrective measures. The malicious actor in the VLC will be detected when there is a change in the output signal of light intensity for communication (in the case of a Sybil attack), a reduction in the total information received (in a delay attack), or several communication attempts which signal a DoS attack. To address the attacks, the vehicles always fetched the control information before acting on any other commands. The priority of the control information prevented the splitting of the vehicles at the intersection.

The security of the platoon after the attack adopted color-shift keying (CSK) through a light-to-frequency (LTF) converter. Furthermore, this system uses a receiver that will decode the symbols with regard to the frequency of transmission. A drop in the RGB intensity of light transmitted in the platoon signals an anomaly. CSK uses coded symbols to transmit the control information from the leader using a microcontroller.

We would like to recommend the following activities and further research to increase the utility of the vehicle platooning. First, the GPS should always be activated to ensure the location of the vehicles with respect to the leader. Secondly, an attack recognition system can be incorporated to increase the probability of detecting an attack.

Acknowledgements

Without the collaborative effort from the two of us, this research could not have been possible. The Qatar University staff ensured that we had access to all the resources we needed, including relevant software licenses, to make this project a success.

References

[1] S. Ucar, S. C. Ergen and O. Ozkasap, "IEEE 802.11p and Visible Light Hybrid Communication Based Secure Autonomous Platoon," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8667–8681, 2018.

[2] T. Cevik and S. Yilmaz, "An overview of visible light communication systems," *International Journal of Computer Networks & Communications*, vol. 7, no. 6, pp. 139–150, 2015.

[3] The National Highway Transportation Safety Administration, 2016 Fatal Motor Vehicle Crashes: Overview, U.S. Department of Transportation, 2017, October.

[4] The World Health Organization, "Road traffic injuries," WHO, 7 February 2020. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries. [Accessed 27 April 2021].

[5] S. Chen, J. Hu, Y. Shi, Y. Peng, J. Fang, R. Zhao and L. Zhao, "Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G," *IEEE Communications Standards Magazine*, vol. 1, no. 2, pp. 70–76, 2017.

[6] B. Han, S. Peng, C. Wu, X. Wang and B. Wang, "LoRa-based physical layer key generation for secure v2v/v2i communications," *Sensors*, vol. 20, no. 3, p. 682, 2020.

[7] 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.

[8] K. A. Rahman and K. E. Tepe, "Towards a cross-layer based MAC for smooth V2V and V2I communications for safety applications in DSRC/WAVE based systems," in *2014 IEEE Intelligent Vehicles Symposium Proceedings*, 2014, June.

[9] S. Kim and R. Shrestha, Automotive Cyber Security: Introduction, Challenges, and Standardization, Springer Nature, 2020.

[10] X. Liu and A. Jaekel, "Congestion control in V2V safety communication: Problem, analysis, approaches," *Electronics*, vol. 8, no. 5, p. 540, 2019.

[11] H. Hasrouny, A. E. Samhat, C. Bassil and A. Laouiti, "A security solution for V2V communication within VANETs," in *Wireless Days (WD)*, 2018.

[12] H. Hasrouny, C. Bassil, A. Samhat and A. Laouiti, "Group-based authentication in V2V communications," in *Proceedings of IEEE Fifth International Conference on DICTAP*, 2015.

[13] H. Hasrouny, C. Bassil, A. Samhat and A. Laouiti, "Security Risk Analysis of a Trust model for Secure Group Leader-based communication in VANET," in *Ad-hoc Networks for Smart Cities*, Springer, 2016, pp. 71–83.

[14] H. Hasrouny, A. E. Samhat, C. Bassil and A. Laouiti, "VANET security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[15] W. Whyte, A. Weimerskirch, V. Kumar and T. Hehn, "A security credential management system for V2V communications," in *IEEE Vehicular Networking Conference*, 2013.

[16] H. Hasrouny, A. E. Samhat, C. Bassil and A. Laouiti, "Trust Model for Group Leader Selection in VANET," in *The 4th International Conference on CSCEET*, 2017, April.

[17] S. Rehman, M. A. Khan, T. A. Zia and L. Zheng, "Vehicular Ad-Hoc Networks (VANETs) – An Overview and Challenges," *Journal of Wireless Networking and Communications*, vol. 3, no. 3, pp. 29–38, 2013.

[18] C. Smith, The car hacker's handbook: a guide for the penetration tester, No Starch Press, 2016.

[19] X. Lin and R. Lu, Vehicular ad hoc network security and privacy, Piscataway: IEEE Press, 2015.

[20] J. Stapleton, Security without Obscurity: A Guide to Confidentiality, Authentication, and Integrity, CRC Press, 2014.

[21] I. A. Sumra, I. Ahmad and H. Hasbullah, "Classes of attacks in VANET," in *2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC)*, 2011, April.

[22] B. Aslam, P. Wang and C. Zou, "An economical, deployable, and secure architecture for the initial deployment stage of vehicular ad-hoc network," in *Secure System Design and Trustable Computing*, C. Chang and M. Potkonjak, Eds., Springer International Publishing, 2020, pp. 487–520.

[23] J. P. Aumasson, Serious cryptography: a practical introduction to modern encryption, No Starch Press, 2017.

[24] 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.

[25] D. Su and S. Ahn, "Autonomous platoon formation for VANET-enabled vehicles," in *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, 2016, October.

[26] H. Hexmoor, S. Alsamaraee and M. Almaghshi, "Blockchain for improved platoon security," *International Journal of Information*, vol. 7, no. 2, pp. 1–6, 2018.

[27] E. Z. Madeleine, B. Dafflon, F. Gechter and J. M. Contet, "Vehicle platoon control with multi-configuration ability," *Procedia Computer Science*, vol. 9, pp. 1503–1512, 2012.

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

[29] J. Liu, D. Ma, A. Weimerskirch and H. Zhu, "Secure and safe automated vehicle platooning," *IEEE Transactions on Reliability*, 2016.

[30] A. Yasser, M. Zorkany and N. A. Kader, "VANET routing protocol for V2V implementation: A suitable solution for developing countries," *Cogent Engineering*, vol. 4, no. 1, 2017.

[31] S. Uçar, S. Ç. Ergen and Ö. Özkasap, "Visible light communication in vehicular ad-hoc networks," in *24th Signal Processing and Communication Application Conference (SIU)*, 2016, May.

[32] T. Rosenstatter and C. Englund, "Modelling the level of trust in a cooperative automated vehicle control system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 4, pp. 1237–1247, 2017.

[33] S. Zhao, T. Zhang, N. Wu, H. Ogai and S. Tateno, "Vehicle to vehicle communication and platooning for EV with wireless sensor network," in *54th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, 2015, July.

[34] G. S. Ramchurn, S. Dhoundiyal, A. R. Signh and B. Maji, "Digital beamforming techniques – A comparison," in *Advances in Communication, Devices and Networking: Proceedings of ICCDN 2017*, Springer, 2018, pp. 701–710.

Biographies

Daniel Kyalo Ndambuki is a professional telecommunication engineer with B. Eng qualification in electrical and telecommunication engineering from Moi University, Kenya. He is also a researcher in offensive cyber security and pursuing MSc. In Telecommunication Engineering Degree.

Hitmi Khalifa Alhitmi is a Qatar-born academician with interests in smart traffic light system. He invented and patented smart traffic light system, which applies artificial intelligence system to determine the equilibrium time needed for each traffic light. The system also reduces accident rates by providing a pre-warning system. His other academic achievements include MSc. Degree in Marketing Management, BSc International Economics and Business and Marketing. He is currently pursuing PhD in Business and Economics at the University of Edinburgh, Scotland.