Journal of Robotics and Control (JRC)
Volume 6, Issue 2, 2025
ISSN: 2715-5072, DOI: 10.18196/jrc.v6i2.25243

Analysis and Design of a Robust Security System to Address Cybersecurity Vulnerabilities and Control the Security of the Internet of Vehicles

Rafah Kareem Mahmood [1*], Salam Waley Shneen [2], Dhurgham Abdulridha Jawad Al-Khaffaf [3]
[1] Electromechanical Engineering Department, University of Technology, Baghdad, Iraq
[2] Energy and Renewable Energies Technology center, University of Technology, Baghdad, Iraq
[3] Laser and Optoelectronics Engineering Department, Engineering Technical College/Najaf, Al-Furat Al-Awsat Technical University, Kufa, Iraq
Email: [1] 50150@uotechnology.edu.iq, [2] salam.w.shneen@uotechnology.edu.iq, [3] cot.drgham1@atu.edu.iq
*Corresponding Author

***Abstract*—The Internet of Vehicles (IoV) system faces some security vulnerabilities, which could lead to cyberattacks targeting smart vehicles. This paper investigates the cybersecurity challenges of IoV, focusing on defending smart cars from covert attackers. The primary aim of the study is to design a robust security system to combat and prevent these cyber-attacks. The work makes two main contributions: First, it explores the security vulnerabilities in inter-vehicle communication, particularly focusing on two types of cyber attacks. To address these vulnerabilities, an intelligent detection algorithm is proposed to close security gaps within the system. The study also discusses the role of smart vehicles and their interconnected systems, which communicate through the Controller Area Network (CAN) bus and other external communication units. Second, the study emphasizes the importance of protecting critical vehicle systems such as the engine control unit (ECU), adaptive cruise control (ACC), anti-lock braking system (ABS), and central locking system. These systems are crucial for vehicle safety, and any compromise could have disastrous consequences. The proposed approach utilizes a Proportional-Integral-Derivative (PID) controller to monitor and control acceleration, leveraging real-time measurements of speed and distance to prevent accidents and mitigate security risks. The results demonstrate the ffectiveness of the proposed solution in securing smart vehicles from cyber threats, by ensuring safe dynamic vehicle systems under potential cyber-attacks.**

Keywords—Interference Detection; Internet of Vehicles; Ad-Hoc Security; Cyber Security; Vehicle-to-Vehicle Communications; Smart Cars; Covert Attacks.

I. INTRODUCTION

Internet-networks are used in many fields such as security systems for detecting cyber-attacks. One of applications is secured vehicle traffic in directions. Electromechanical systems are those systems that have an electrical system and a mechanical system. Therefore, if we want to represent the electromechanical system, we will need to represent the electrical part and the mechanical part physically and mathematically. The movement in which vehicles rotate is involved because it needs a machine to provide it. The electrical systems need the electrical supply sources whose output is regulated and controlled according to appropriate reference values that provide the required performance of the proposed system. In network systems, the security systems are available for these systems as well as the control units that suit their inputs and outputs by specifying the necessary data to enable the expected attack to be detected when any change occurs. Smart vehicles, which include land such as smart cars (sea and air), are applications of these systems. Smart vehicles should have the protection systems to prevent disasters that may be caused by any system intrusion. This requires to develop early detection systems, controlling the process of repelling attacks and preventing them from penetrating the system [1]-[5]. The process of controlling and controlling through managing and organizing the traffic of smart vehicles is of interest through working on preparing contributions that include, first, creating a number of innovative solutions with the aim of identifying and alleviating congestion, and second, developing a procedure to improve and raise the efficiency of the performance of transportation systems. The process of employing and using some data collected from the real environment and providing beneficiaries with that data may include road options and alternative routes using GPS systems to determine location and road maps in addition to cameras with the aim of reducing travel time in a trip from one place to another and bypassing congested roads. Control units are used in the latest systems and technological techniques of various types, including traditional ones, such as the use of cameras, vehicle speed sensors, and monitoring the environment, including paths, distances, and vehicle deviations from them, etc., with or without a warning signal to the driver. Providing the ability to absorb and analyze the huge amount of data in real time has made workers in various fields of specialization keep pace with the rapid development in technology, such as the field of artificial intelligence, the Internet of Things, and others, important sources to meet the need [6]-[10].

The vehicle operates according to a specific path, and for a group of vehicles, the correct path of vehicle is considered as a private information for each vehicle. When there is a group of vehicles within a faction of smart vehicles, its operation depends on the presence of a command vehicle for the faction. Data is exchanged through a communication process according to an electronic system that can organize the connection during the communication of one vehicle with another or with the platoon leadership; it is called

vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) to implement the correct and required paths for all vehicles. The exchanged data process depends on the speed and location of each vehicle through the communication process with the faction, so that the data reaches all members of the faction according to a system that collects and distributes the reference data for all the faction's vehicles. To provide a vehicle safety according to the correct behavior, that suits the location and speed of each vehicle requires an information security system and protection from cyber-attacks. It is expected within a fragile wireless-communications-systems [11]-[15]. The attack process, including a denial-of-service attack, is based on the data delay process as a result of channel occupancy, which delays the data issued and received within the communication channels that misleads the vehicle from the correct path. Many researches and studies have been conducted and discussed such attacks and their impact on the communication network between smart vehicle communication channels starting with the presence of a service, blocking that service, detecting the attack, and returning the stability and service. Control systems are the basis for dealing with disturbances in the systems and restoring the correct behavior of the system, which required the vehicle path for a faction of smart vehicles. Work is underway to design a controller within a real-time dynamic detection system. The effectiveness of the system can also be verified through stability [9]. The system is considered to be exposed to a packet loss attack, which leads to data loss and delay. The concept is how to deal with it according to the secured-communication-topology by providing a high-gain control base [10]-[20].

Internet-networks are used in many fields such as security systems for detecting cyber-attacks. One of applications is secured vehicle traffic in directions. Electromechanical systems are those systems that have an electrical system and a mechanical system. Therefore, if we want to represent the electromechanical system, we will need to represent the electrical part and the mechanical part physically and mathematically. The movement in which vehicles rotate is involved because it needs a machine to provide it. The electrical systems need the electrical supply sources whose output is regulated and controlled according to appropriate reference values that provide the required performance of the proposed system. In network systems, the security systems are available for these systems as well as the control units that suit their inputs and outputs by specifying the necessary data to enable the expected attack to be detected when any change occurs. Smart vehicles, which include land such as smart cars (sea and air), are applications of these systems. Smart vehicles should have the protection systems to prevent disasters that may be caused by any system intrusion. This requires to develop early detection systems, controlling the process of repelling attacks and preventing them from penetrating the system [21]-[25].

Attacks include the penetration of one of the communication channels associated with the network through an attack in which a secret deception is carried out that could lead to the deterioration of the system if it is not detected. To solve this problem and eliminate a situation of being exposed to any potential attack, an early detection system for any attack must be established. Possible cases of attacks are considered to be the first case of creating an error to cause instability in the system outputs. The second case is the possibility of the attacker to create effects of a transient state and repeat it for long periods. These situations are reflected on the vehicle speed adaptation systems by increasing or decreasing the speed to increase or decrease the distance between vehicles. A model is designed and built to detect the covert attacks. The model is trained to limit the system's response to behavior that deviates from what is scheduled and expected, which requires in presence of a warning and demands to turn to the secure system with compensating of any damage that could affect the effectiveness of the system [26]-[30].

Some conducted studies on the recent works are presented. Detection of attacks on smart vehicles that may cause car accidents and ways to avoid are related. In [1], A threat-modeling method (TMM) is used in order to completely safeguard the intelligent and autonomous-vehicles (IAV) system. Some related taxonomies to autonomous-vehicles are discussed, including the vulnerability, defense, and privacy. Vehicular-ad-hoc networks (VANETs) has been analyzed the connectivity with minimal computation and communication overhead via software-defined networking (SDN) for V2V communication [2][18]. A survey on the security-attacks for VANETs visualized in [17], and the security and privacy issues within vehicular-cloud-computing (VCC) discussed such as features, trust-management-models, problems and threats. The dynamic-digital-twin (DT) for resource-allocation of aerial-assisted IoV exhibited to capture the time-varying source and needs of resources. The authors designed a two-stage incentive mechanism based on Stacker berg game where DT of vehicles/road-side-units (RSUs) deemed as the leader and the RSUs, which provides computing-services to the follower [3]. As in [6], the introduced mathematical-models to improve the road-safety for intelligent-vehicles demonstrated and categorized into physics-based, maneuver-based, and interaction-aware models, with challenges of high costs and real-time assessment issues. Vehicle platooning offered a promising-solution to increasingly traffic-challenge by enabling an efficient traffic-management with minimal vehicle-involvement. In a platoon, a leading-vehicle (LV) is followed by several following-vehicles (FVs), enhancing road efficiency, fuel consumption, and safety [7]. Recent research has introduced algorithms for multi-vehicle-negotiation among autonomous-vehicles (AVs) using dedicated-short-range-communications (DSRC) [8]; four-way-intersection scenario indicated that the approach can reduce the average vehicle delays up to 50%, but it may increase delay-variance and reliability-concerns especially at the interconnected intersections. These findings underscored both the potential challenges of implementing vehicle platooning [9]. Recent work highlighted various solutions to enhance vehicular communication and address the challenges in cooperative-vehicle-infrastructure systems (CVIS), traffic management, and security within the vehicular-internet-of-things (VIoT). The proposed analytical

framework in [10] emphasizes the benefits of cooperative computation for vehicular applications with tight deadlines and large data sizes. In [11], the investigation on smart routing protocol to improve the security against malicious attacks in VIoT networks by authenticating sources and incorporating security metrics lastly grown. Addressing traffic congestion in the smart cities discussed [12], an intelligent transport system utilized IoT to gather traffic data and enhance decision-making using feature selection and machine-learning for improving the accuracy. The study in [13] introduced the application of block-chain-technology in AVs to mitigate cyber-attacks by securing data sharing and utilizing smart contracts to the access control. Moreover, the design in [14] explored the use of deep-learning-algorithms for predicting vehicle density and mobility to enhance the navigation of crowding management in vehicular networks. Lastly, the work in [15] critiqued the existing of vehicular networks for their limitations in scalability and intelligence, proposing software-defined-vehicular-networks (SDVNs) to optimize the performance while addressing security challenges associated with increased mobility and potential attack surfaces. In conjunction, these studies underscored the need for advanced solutions in vehicular communication, traffic management, and security for future smart-city infrastructures. Intrusion-detection-system (IDS) based flow in VANET using context-aware-feature-extraction (CAFE) employed in [16]. A multi-class IDS used convolutional-neural-network (CNN) with CAFE manner. The outcomes revealed that the suggested design had solid identification of hard-to-detect the passive-attacks compared to ordinary machine-learning techniques. Although it represented the difficulties, federated-learning (FL) in IoV can improve the security. The study in [19] depicted a unique paradigm of FL that examined the security on the three dimensions: network reliability, data transmission success rate, and trust. The framework achieves the test accuracies of 85%–90%, according to the simulation data. In [20], named-data-networking (NDN) retrieved the content based on its name rather than an IP-address, focusing on interest-forwarding strategies to address broadcast storms from traditional flooding methods. Various techniques have been developed to mitigate this issue. The proposed mobility-prediction-of-direction-and-timer (MoDT) for interest-forwarding-strategy selectively chosen the forwarders based on link availability time and direction; the superior performance compared to imitative NDN and RA-NDN. A study in [4] developed the static and dynamic scheduling frameworks of AVs to optimize coordination for implementing an electrical-vehicle-energy-management with multi-objective optimization and numerical-simulations. The research in [24] examined the security of ACC systems in smart vehicles against covert attacks by utilizing a P controller. The extensive-simulations were conducted to portray the successful detection of covert attacks in ACC systems and realized the compensator.

To evaluate whether the control system is effective or not, the system needs to conduct the tests of operating conditions similar to the real system. Work is underway to build a simulation model using MATLAB to study the proposed system. The system can be represented by checking the movement of vehicles operated via an electric motor and determining the required speed for a normal situation without attacks. In order to control the required and appropriate behavior for the system, it is necessary to develop the other examined cases that present the potential attacks such as transient cases, errors, and system instabilities and the treatment through early detection of attacks with fast response system.

This study introduces three scenarios of smart of vehicles/cars. The output of ACC system is identified as a stable-status at the first. Subsequently, the transient-case is determined via changing the ACC outputs, which is compared to the normal-situation. This caused by potential covert attacks where the attacker attempts to dominate some portions of cyber-physical-system. The classical ACC controller trains to avoid errors with immediate response to get around this issue. Finally, artificial-intelligent-algorithm with neural-network-identifier are offered to control on space and speed. The rest of our presented research has been outlined as follows: Section 2 characterizes the motivation and main aims of our presented work. The system plans and how the modeling is built are discussed in the section 3. The mathematical model of ACC and the system dynamics are reported in the section 4. The intrusion-detection-algorithm and the compensator of simulation setting are portrayed in the section 5. The essential points are drawn in the section 6.

II. MOTIVATION AND OBJECTIVES

Protecting people's lives from traffic accidents requires thinking about using smart and advanced systems such as smart cars. Smart and advanced vehicular systems need the control and security systems. Working to build an integrated system to provide a security system based on transmitting and receiving data that helps to know the surrounding environment and deal with changing conditions. This requires modern technologies and provides the vehicle's connection with the outside world, which is connected with other vehicles. The systems are connected to internal and external network. In the most systems that operates according to a network system, they may be exposed to an electronic attack and may be exposed to a lockout of the central system. Thus, vehicle systems may be prevented from working in the correct and safe manners such as the inability to brake the vehicle or control the speed, which may cause the traffic accidents. Therefore, the rules must be established to suit the control systems and security system to protect the vehicles from any expected attack to ensure the safety of the vehicle.

The primary goal of the current study is to work on the underway developments of proposal to detect the intrusion and attack on the system by ensuring speed control and setting the necessary compensation as a result of alterations in the environment and surrounding conditions. Within this field, there is a secret cyber-attack that could be threaten the movement system of land (sea or air) vehicles. The working environment must be studied by determining the inputs and outputs of the system with different operating conditions. The security and control systems require a dynamic comparison of the system's outputs through the normal condition with other abnormal effects that can be detected as

a result of any change. Detection systems stimulate the control systems to address these conditions.

It is possible to create a system model that simulates what has been proposed and conducted the tests, which suits to the real work environment by using the computer program MATLAB to verify the possibility of processing and evaluating the effectiveness of the system [57]-[59]. It is feasible to improve and develop the performance of control units with smart and expert systems.

III. DESCRIBE THE SYSTEM AND BUILD THE MODEL

It is possible to choose a vehicle somewhere on the roads, and it is also probable to drive on an empty road in absence of a vehicle. This virtual state is considered to exist in the real distance, but it is potential for other vehicles to appear at any moment from both sides of the road on the right or left. There is no doubt that requires a safe distance between vehicles. Therefore, we need to determine the distance, speed, and the direction of movement, which finds a number of surrounding vehicles. This system is linked to a network that collects information from all vehicles and also gives it to all vehicles to determine the required and safe speeds and distances among vehicles.

The safety system needs to control the vehicle's movement speed by regarding the safe-distance. Therefore, the vehicle's speed is linked to the velocity of nearby vehicles according to the conditions of safe distance. The smaller or larger distance is determined to enable the control systems to address potential errors. One of the important rules of the safe system for driving smart vehicles is to adjust the speed control system to maintain the safe distance and not to approach any two vehicles less than the smallest safe distance. The system can be labeled as mode number one, when it is being in a safe mode and mode number two, when it is being in an unsafe mode. The processing systems are activated when the system detects mode number two and is able to handle the error of the system to return to mode number one.

In order to build the model, the necessary symbols for the elements of the system can be determined through their association with each other in performing a particular activity. The appropriate mathematical model can be drawn by a flow chart as shown in Fig. 1 to build the model in order to conduct the proposed tests and observe the different states of the system.

The model is dynamic for vehicles including the vehicle velocity, vehicle position, and vehicle acceleration. The collected data for all vehicles can enable the control unit to follow the stable-state and determine position number one in order to avoid any disturbance in the system. A speed control system can be developed by using Proportional Integral Derivative (PID) controller. The appropriate function can be written and the speed and acceleration encoded. The position and velocity in the flow chart is expressed the control of the vehicle's cruise on the road according to the driving behaviors that suit the information taken from the sensors linked to the system management network.

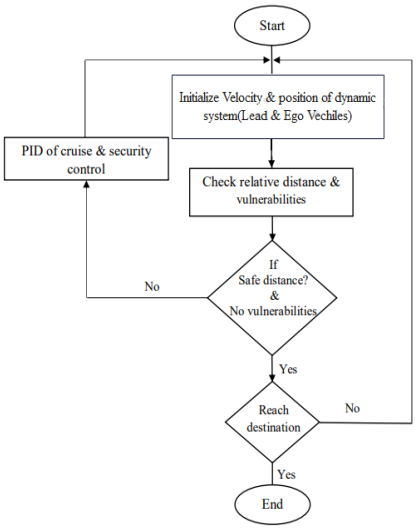


Fig. 1. The Flow Chart of built security cruise control system

IV. MATHEMATICAL OF THE DYNAMICS MODEL

To work on laying the correct foundations that suit the specifications of any system of this type, it is necessary to identify the components of the system and the surrounding environment. One of the system assumptions is that the internal components of the network that are designed in the field of smart and modern vehicles are adopted. The network includes sensors and must be characterized by high accuracy and provide effective remote communication systems in addition to the vehicle's transmission system. The system parts are connected through a network inside the vehicle in addition to control protocols that are added to effective communication technologies to address security vulnerabilities, which limits attackers' access to the internal network of smart vehicles. After representing the acceleration model, it can also be pointed out that it is not conceivable to move from one speed to another with except the gradual manner, and this depends on the laws of motion to be written in the mathematical equation. A model can be represented for each vehicle and it depends on the number of vehicles connected to the network, to be modeled. As a result, the difference in speed and position of the vehicle is according to the data of each vehicle. The Laplace transform can be performed to represent the model with the transformation function that is used to perform system tests.

The complexity of systems increases with the increase in the number of their components, which increases the amount of data exchanged between them. System analysis and design require effective, accurate and highly efficient control units to achieve all the different requirements of the system's functions. Among the variables that are of interest are the time periods for exchanging data to implement it in addition to its bandwidth, which provides comfort and security. It is possible to develop a model for the system components to identify its stages and functions in addition to the units associated with the system.

A system based on cyber security for vehicles is evaluated by proposing the determination of both the speed set at a certain time and the appropriate location for that speed, which achieves the process of improving the performance of the system and the traffic efficiency of smart

vehicles that need a comfort protection system with the possibility or just the case of an attack by attackers with private and critical data, which may pose a threat to the lives of drivers, passengers and their vehicle.

The contributions of the study can be made by defining and presenting a simulation model in which a communication network is presented with technologies including protocols and controllers and setting appropriate security assumptions with the encryption mechanism and machine learning required in vehicle cybersecurity.

To simulate the system, it is necessary to define the measurement criteria for the system behavior and express the different states that accompany the proposed system. The time distance and the metric distance are two important elements to provide cyber security, i.e. determining the appropriate time to avoid accidents with the appropriate safety distance. Exposure to attack or not, this is the basic assumption for the system to work, so the behavior is different for the two cases. The network detects a potential attack state according to the system data, which indicates the possibility of the network being exposed to an attack. The system state is normal when there is no attack, no action is required from the system according to the data the system is simulating for this case. While the system state differs when there is a possibility of an attack, i.e. the data specified for the system state changes through a matching process for the two basic system states.

To simulate the system, it is necessary to define the measurement criteria for the system behavior and express the different states that accompany the proposed system. The time distance and the metric distance are two important elements to provide cyber security, i.e. determining the appropriate time to avoid accidents with the appropriate safety distance. Exposure to attack or not, this is the basic assumption for the system to work, so the behavior is different for the two cases. The network detects a potential attack status according to the system data, which indicates the possibility of the network being attacked. The system status is normal when there is no attack, no action is required from the system according to the data the system is simulating for this case. While the system status differs when there is a possibility of an attack, i.e. the data specified for the system status changes through a process that matches the two basic system states. From the commands and instructions that depend on the data and give a message to direct the vehicle in directions including the right, left or middle, and it can also take the criterion of the far left or the far right. There is another message in the system that contains data about the vehicle's braking status with criteria including high, low, medium, or no brake pressure, in addition to messages and criteria including RPM, gear, radar, coolant, speedometer, acceleration, and others such as engine temperature and whether or not it has been attacked.

In this section, there are two types of vehicles such as lead and ego vehicles. Ego has a radar to calculated the range to lead-car. Both vehicles are in same road. The relative-speed is computed via radar/sensor units. ACC goals are to keep the safe-distance between vehicles as visualize in Fig. 2. ACC system either controls the speed of ego-vehicle or maintains the space between vehicles also by controlling the velocity. Different speeds can be realized by considerably accelerating or decelerating. ACC system works in the close-loop.

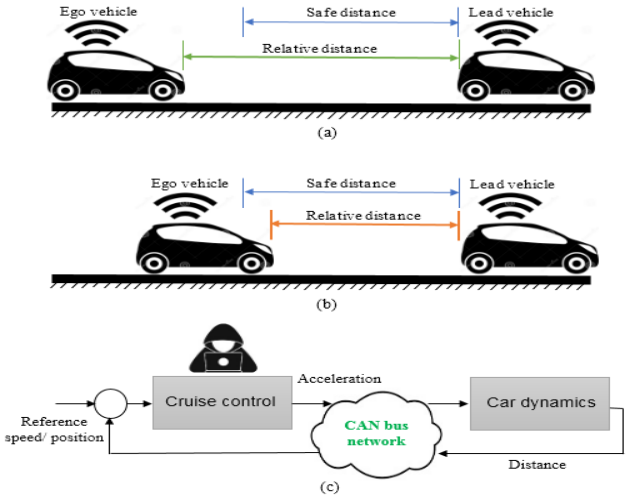


Fig. 2. Description of ACC system with various operational modes and controls on the distances as in (a) Drel ≥ Dsafe (b) Drel < Dsafe and (c) closed-loop ACC system

The system can be mathematically represented as in equations (1) and (2) and includes the system dynamics model as in equation (3) all the way to representing the system with a transfer function after performing the Laplace transformation and conducting system tests for the model. By studying the behavior of the system, the performance can be improved, and it is possible to poison a suitable and efficient control system.

A test case can be selected that represents the system being attacked. An intelligent system can also be designed to detect the attack. The change is resulted from the system disturbance to be compensated by setting a speed and position controllers and adjusting the system outputs according to the reference values.

The relationships can be written by indicating to position, speed of vehicles and acceleration ($v = \dot{x}. a = \dot{\upsilon} = \ddot{x}$), where v, a, $\dot{x}$ and $\ddot{x}$ are velocity, acceleration, first-order model and second-order mode, respectively. The vehicle-cruise-control dynamic model with respect to space-form is calculated as in:

$$\dot{x}_{ego}(t) = F_v\big(D_{rel}(t)\big) \quad (1)$$

$$D_{rel}(t) = x_{lead}\,(t) - x_{ego}(t) \quad (2)$$

The second-order design are described in Newton's law of motion, as expressed

$$\ddot{x}_{ego} = F_a\big(x_{lead} - x_{ego}.\dot{x}_{lead} - \dot{x}_{ego}.\dot{x}_{ego}\big) \quad (3)$$

Where D is the distance, D_{safe} is the safe-distance; D_{rel} denotes the relative-distance, v is the velocity, F is a function, F_v shows the velocity-function, x is the position, a is the acceleration, $x_{ego}(t)$ is the position of ego-vehicle, $x_{lead}(t)$ is the position of lead-vehicle and F_a is the acceleration-function of ego-vehicle.

Equation (1) refers to the vehicle speed representation with the control unit, include relationship velocity of ego vehicle with velocity function and relative distance. Also, equation (2) assigns the relative-distance with position of ego-vehicle and position of lead-vehicle. Equation (3) can be written to indicate the nonlinear state model of the acceleration system and includes the relationship between acceleration of the ego-vehicle with position of ego and position of lead vehicle. Furthermore, the second-order model optimal-velocity is computed as follows.

$$\ddot{x}_{ego} = \alpha \times \frac{v_{rel}}{D_{rel}} \tag{4}$$

$$\ddot{x}_{ego} = \alpha \times \frac{\dot{x}_{lead} - \dot{x}_{ego}}{x_{lead} - x_{ego}} \tag{5}$$

Where v_{rel} is the relative-speed to the lead-car, which got it via vehicle-radar. Also, the optimal-velocity-model is given as

$$\ddot{x}_{ego} = \beta \times \left(F_v\left(\dot{x}_{lead} - \dot{x}_{ego}\right) - \dot{x}_{ego}\right) \tag{6}$$

By combing Eq. (5) and Eq. (6), we will get

$$\ddot{x}_{ego} = \alpha \times \frac{\dot{x}_{lead} - \dot{x}_{ego}}{x_{lead} - x_{ego}} + \beta \times \left(F_v\left(\dot{x}_{lead} - \dot{x}_{ego}\right) - \dot{x}_{ego}\right) \tag{7}$$

Where α and β are constant parameters. As aforementioned, the dynamic-model among acceleration and speed for both ego and lead is exactly same system (linear-time-invariant) in the second-order. Thus, the mathematical transfer-function between the velocity and acceleration for lead-ego vehicles can be expressed in Laplace-domain as written

$$G(s) = \frac{1}{\frac{s^2}{2} + s} \tag{8}$$

Which is roughly represented the choke-body and car-inertia. The safe-distance between lead-car and ego-car is calculated as:

$$D_{safe} = D_{default} + \left(T_{gap} \times V_{ego}\right) \tag{9}$$

Where Tgap and V_{ego} denote the gap between lead-ego vehicles and ego-vehicle-velocity. The driver-set-velocity (V_{set}) is considered as the input of ACC while the output of ACC can accelerate the ego-vehicle.

V. SYSTEM EVALUATIONS AND DISCUSSIONS

In this part, we will experiment the model by using transfer-function. Our introduced ACC system have mathematically represented where will be prone to maleficent hackers. The suggested strategies for smart-vehicles are applied for both detection and compensation. The configurations of our simulated ACC system are clarified in Table I.

Firstly, the system is examined without any attack to study the behavior of the system in the normal-situation in order to train/identify the traditional PID controller with whole cases on the stable-state of the system, as revealed in Fig. 3. Then, it is easy to determine the appropriate data for the system's input and output.

TABLE I. ILLUSTRATION OF THE DESIGNED MODEL PARAMETERS [60]

Symbols	Values	Units
X_0, lead	50	m
X_0, ego	10	m
V_0, lead	25	m/s
V_0, ego	20	m/s
T_{gap}	1.4	s
$D_{default}$	10	s
V_{set}	30	m/s
a_{ego}, min	-3	m/s2
a_{ego}, max	2	m/s2

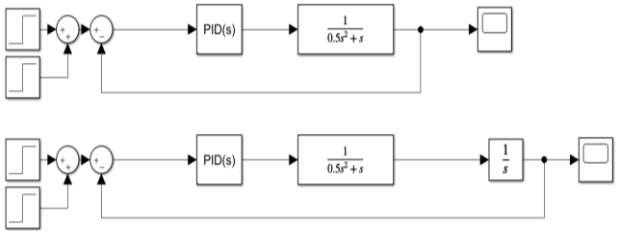


Fig. 3. First scenario of default ACC smart cars control system to know the security vulnerabilities and learn the steady-state

It is obviously demonstrated that ACC controller increase the velocity at constant and regular intervals, as reported in Fig. 4(a). Consequently, the position response will be changed according to speed with keeping a safe-distance from others to prevent disasters, as denoted in Fig. 4(b). Secondly, the system is tested with a non-recurring error as presented in Fig. 5; A transient state is immediately detected a potential attack, which changes the state of the system. The system discovers abnormal pattern, which attempts to vary the system's behavior. We will study this state of the system with returning to the stable-state by helping of the control unit of traditional controller with rapid response.

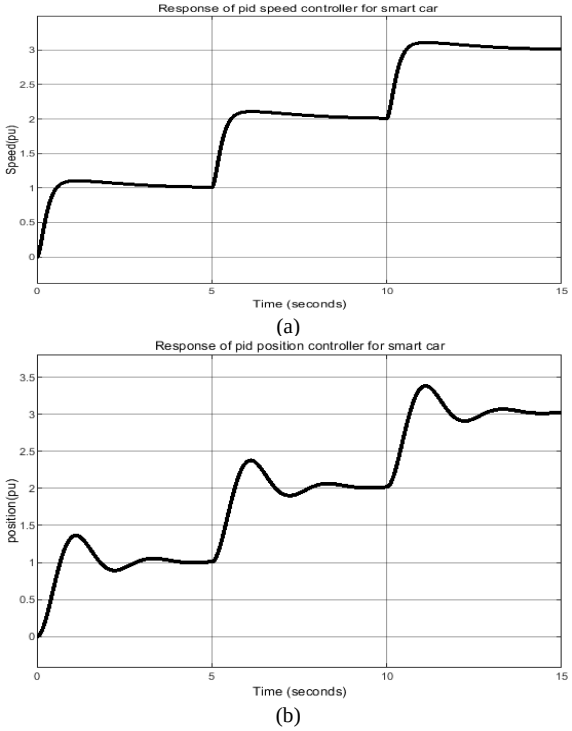


Fig. 4. First scenario response findings for both (a) velocity vs. time and (a) position vs. time in the smart cars

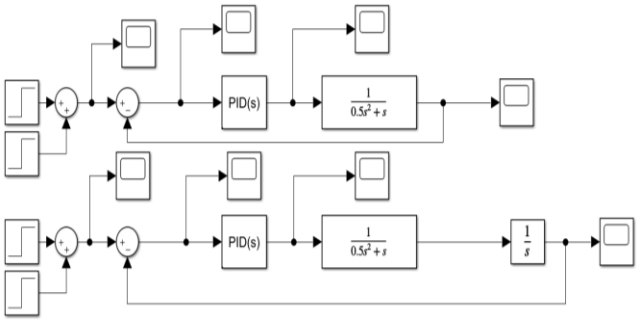
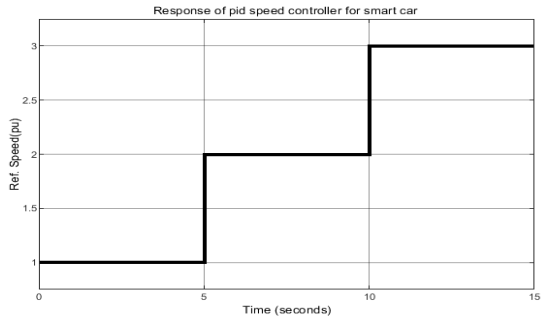
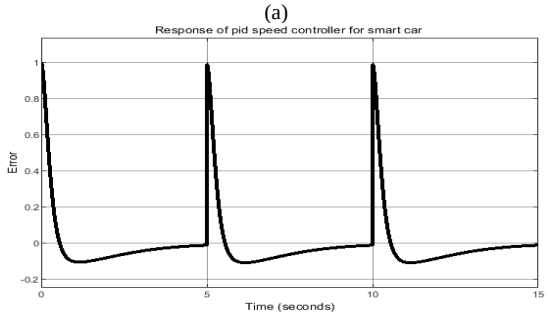


Fig. 5. Second scenario of intelligent vehicles after susceptible attacks

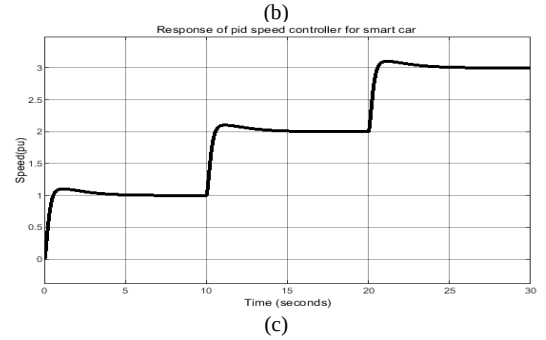
Fig. 6(a) depicts that the reference speed signal is produced in order to compare with actual speed as in figure 6.c. There are errors founded in terms of Fig. 6(b) and Fig. 6(d). The vehicle-space is gradually grown due to the transient-situation resulted from the covert-attacks, as exhibited in Fig. 6(e). A malicious control on ACC system is intended to rise the probability of the collision. PID system is enabled after launching the attack, which attempts to accelerate the velocity of ego-vehicle and minimize the speed of lead-vehicle in order to lower the safe distance less than threshold. A such manipulation is un-noticeable via driver. In this way, the chance of accidents will be proliferated. However, smart-vehicles must be equipped with a radar and sensors to build a network with nearby cars to create a database to limit the distance and speed to avoid collision.



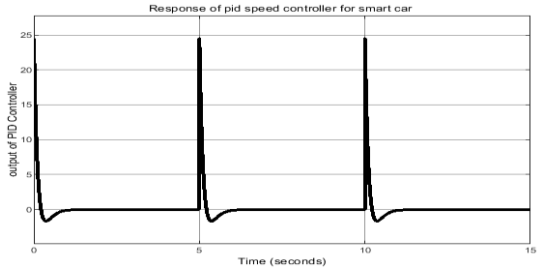
(a)



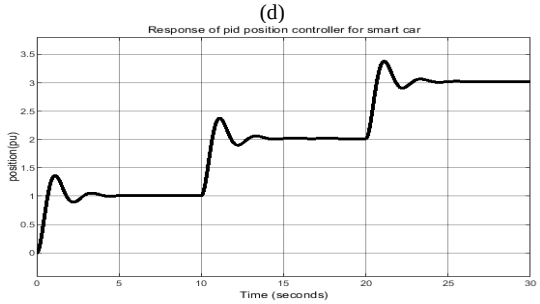
(b)



(c)



(d)



(e)

Fig. 6. Intrusion-detection for attack scenario (a) reference speed values over time (b) the observation of error measurements over time via attack (c) the speed measurements of produced PID controller to reduce the acceleration caused by hackers (d) PID managements to mitigate the errors at the output of controller and (e) position responses of PID controller for smart automobiles

Thirdly, the expected state is the repetition of the transient state. Therefore, more than one method of controls can be chosen and the best one can be determined through measuring performance and designing the appropriate controller, such as using an expert controller, as portrayed in Fig. 7.

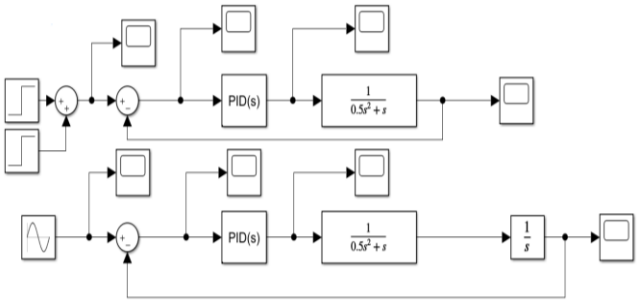


Fig. 7. The schematic paradigm of suggested model for third scenario

Fig. 8(a) and Fig. 8(b) display that there is up-normal beginning in the position controller caused by cyber-attacker compared with actual position. Attacker seeks to tamper the reference-signal of ACC system, which will alter the gap between cars to make it less than safe-distance. The driver does not have a sense of fluctuation in the speed. As a result, the relative-distance (Drel) is gradually incremented and the effective-gap is decreased. This will rise the chance of collision. However, the ACC system changes the operational mode based on the intelligent designed algorithm tries to go back the speed to the ordinary condition. Fig. 8(c) shows the errors at the output of position controller. Here, the role of the PID compensator appears with respect to the reference-position in order to overwhelm the flaws.

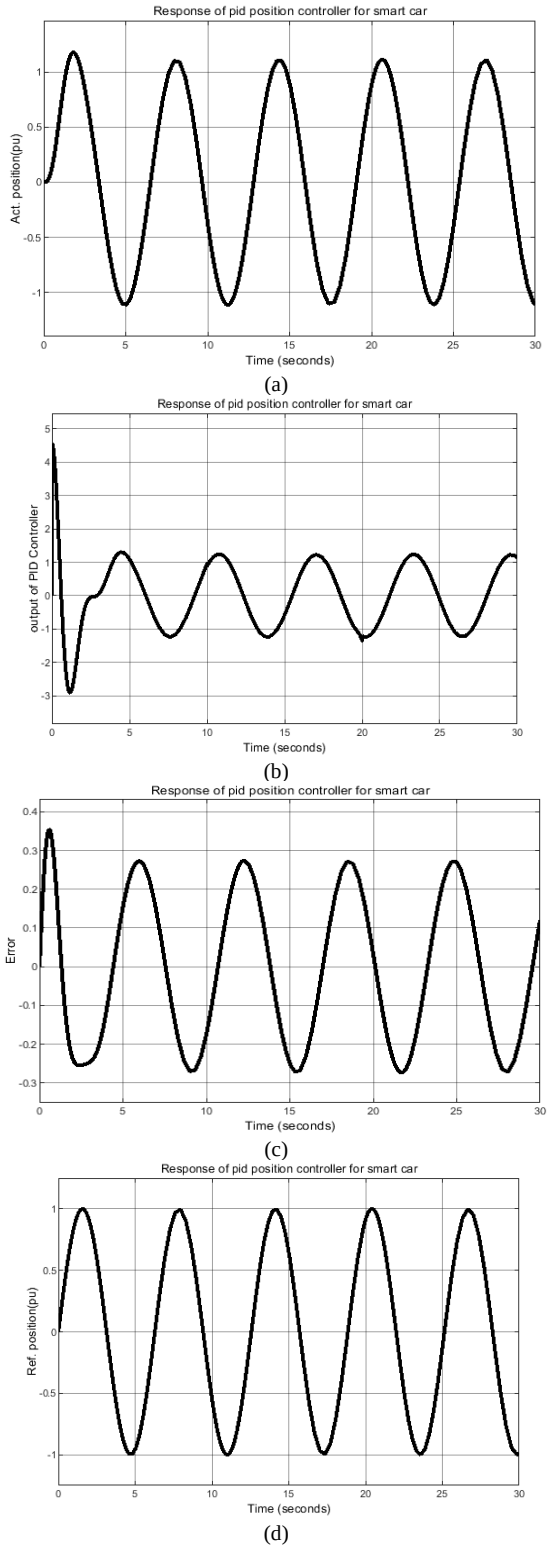


Fig. 8. Third scenario of smart automobiles for (a) the actual position vs. time (b) output response alteration of PID position controller over time (c) error measurements through the time (d) reference position across the time

Fig. 9 visualizes the differences between the references with true speed and position. These changes are occurred in presence of the attack. We infer that the effectiveness of the introduced detection algorithm to expose the hackers in short time at small transient manipulation. The designed PID controller has been proven to deter the attackers with high and rapid responses.

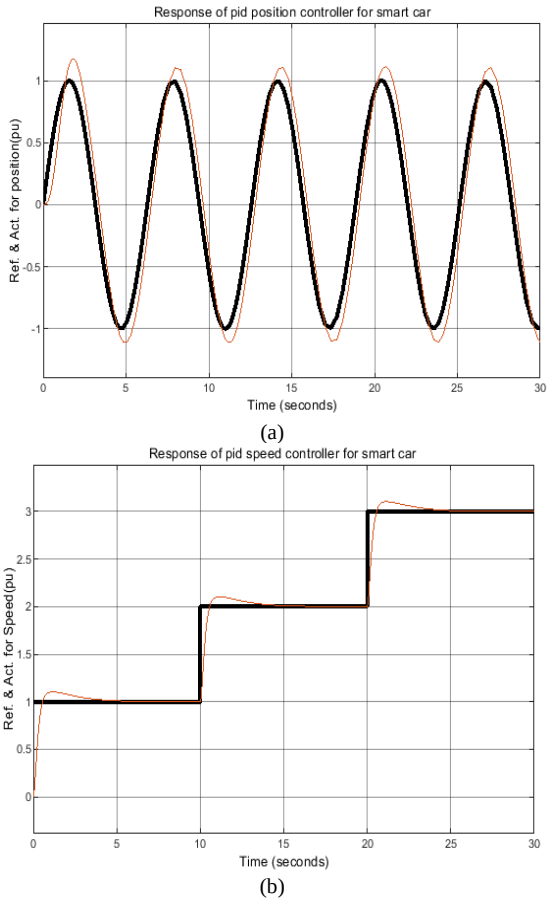


Fig. 9. Performance comparison of reference and actual (a) position and (b) speed after detecting the attack and running the compensation-strategy to recover the malicious hackers applied on ACC unit

VI. CONCLUSION

This research successfully analyzed the cybersecurity challenges of Internet of Vehicles (IoV) technology, with a specific focus on identifying vulnerabilities and mitigating the risks posed by covert cyber-attacks. By utilizing velocity and position as key performance indices, we evaluated the effectiveness of the Adaptive Cruise Control (ACC) system. Through simulation using MATLAB Simulink, three scenarios were explored to address covert cyber-attacks. An intelligent detection algorithm was developed, allowing the ACC system to predict and evaluate its performance, with a comparator used to compare actual outputs against expected ones. Covert attacks were identified using statistical analysis, triggering a transition from a model-predictive controller (MPC) to a Proportional-Integral-Derivative (PID) controller to ensure system security. The simulation results confirmed the effectiveness of the proposed design in reducing the risks associated with covert attacks, particularly in terms of speed and position. The ACC models proposed in this study offer a robust and secure solution, making them ideal for future smart vehicles and suitable for autonomous driving systems, such as Google's self-driving cars.

REFERENCES

[1] S. Kim *et al*., "Security and privacy in intelligent autonomous vehicles," *Automotive Cyber Security: Introduction, Challenges, and Standardization*, pp. 35-66, 2020, doi: 10.1007/978-981-15-8053-6_3n.

[2] N. H. Hussein *et al*., "A comprehensive survey on vehicular networking: Communications, applications, challenges, and upcoming research directions," *IEEE Access*, vol. 10, pp. 86127-86180, 2022, doi: 10.1109/ACCESS.2022.3198656.

[3] K. Kuru and W. Khan, "A framework for the synergistic integration of fully autonomous ground vehicles with smart city," *IEEE Access*, vol. 9, pp. 923-948, 2020, doi: 10.1109/ACCESS.2020.3046999.

[4] R. Amin, I. Pali, and V. Sureshkumar, "Software-defined network enabled vehicle to vehicle secured data transmission protocol in VANETs," *Journal of Information Security and Applications*, vol. 58, p. 102729, 2021, doi: 10.1016/j.jisa.2020.102729.

[5] R. Hult *et al*., "Coordination of cooperative autonomous vehicles: Toward safer and more efficient road transportation," *IEEE Signal Processing Magazine*, vol. 33, no. 6, pp. 74-84, 2016, doi: 10.1109/MSP.2016.2602005.

[6] A. Finn and S. Scheding, "Developments and challenges for autonomous unmanned vehicles," *Intelligent Systems Reference Library*, vol. 3, pp. 128-154, 2010, doi: 10.1007/978-3-642-10704-7.

[7] M. S. Sheikh, J. Liang, and W. Wang, "Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey," *Wireless Communications and Mobile Computing*, vol. 2020, no. 1, p. 15129620, 2020, doi: 10.1155/2020/5129620.

[8] A. Balador *et al*., "A survey on vehicular communication for cooperative truck platooning application," *Vehicular Communications*, vol. 35, p. 100460, 2022, doi: 10.1016/j.vehcom.2022.100460.

[9] K. B. Y. Bintoro, "A study of V2V communication on VANET: characteristic, challenges and research trends," *JISA (Jurnal Informatika dan Sains)*, vol. 4, no. 1, pp. 46-58, 2021, doi: 10.31326/jisa.v4i1.895.

[10] R. Moghaddass *et al*., "Smart control of fleets of electric vehicles in smart and connected communities," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6883-6897, 2019, doi: 10.1109/TSG.2019.2913587.

[11] E. Benalia, S. Bitam, and A. Mellouk, "Data dissemination for Internet of vehicle based on 5G communications: A survey," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 5, p. e3881, 2020, doi: 10.1002/ett.3881 doi: 10.1002/ett.3881.

[12] S. Samarakoon *et al*., "Distributed federated learning for ultra-reliable low-latency vehicular communications," *IEEE Transactions on Communications*, vol. 68, no. 2, pp. 1146-1159, 2019, doi: 10.1109/TCOMM.2019.2956472.

[13] W. Sun *et al*., "Dynamic digital twin and distributed incentives for resource allocation in aerial-assisted internet of vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5839-5852, 2021, doi: 10.1109/JIOT.2021.3058213.

[14] G. Nencioni, R. G. Garroppo, and R. F. Olimid, "5G multi-access edge computing: A survey on security, dependability, and performance," *IEEE Access*, vol. 11, pp. 63496-63533, 2023, doi: 10.1109/ACCESS.2023.3288334.

[15] K. Katsaros *et al*., "AI-Native Multi-Access Future Networks-The REASON Architecture," *IEEE Access*, vol. 12, pp. 178586-178622, 2024, doi: 10.1109/ACCESS.2024.3507186.

[16] S. Lefèvre, D. Vasquez, and C. Laugier, "A survey on motion prediction and risk assessment for intelligent vehicles," *ROBOMECH journal*, vol. 1, pp. 1-14, 2014, doi: 10.1186/s40648-014-0001-z.

[17] T. Limbasiya *et al*., "A systematic survey of attack detection and prevention in connected and autonomous vehicles," *Vehicular Communications*, vol. 37, p. 100515, 2022, doi: 10.1016/j.vehcom.2022.100515.

[18] X. Wang, Y. Sun, and D. Ding, "Adaptive dynamic programming for networked control systems under communication constraints: A survey of trends and techniques," *International Journal of Network Dynamics and Intelligence*, pp. 85-98, 2022, doi: 10.53941/ijndi0101008.

[19] A. Balador *et al*., "A survey on vehicular communication for cooperative truck platooning application," *Vehicular Communications*, vol. 35, p. 100460, 2022, doi: 10.1016/j.vehcom.2022.100460.

[20] O. Dokur and S. Katkoori, "Internet of Vehicles-Based Autonomous Vehicle Platooning," *SN Computer Science*, vol. 5, no. 1, p. 80, 2023, doi: 10.1007/s42979-023-02391-y.

[21] M. Bashiri and C. H. Fleming, "A platoon-based intersection management system for autonomous vehicles," *2017 IEEE Intelligent Vehicles Symposium (IV)*, pp. 667-672, 2017, doi: 10.1109/IVS.2017.7995794.

[22] J. Zhou, D. Tian, Y. Wang, Z. Sheng, X. Duan, and V. C. M. Leung, "Reliability-Optimal Cooperative Communication and Computing in Connected Vehicle Systems," in *IEEE Transactions on Mobile Computing*, vol. 19, no. 5, pp. 1216-1232, 2020, doi: 10.1109/TMC.2019.2907491.

[23] R. Kumar, S. K. Singh, D. K. Lobiyal, S. Kumar, and S. Jawla, "Security Metrics and Authentication-based RouTing (SMART) Protocol for Vehicular IoT Networks," *SN Computer Science*, vol. 5, no. 2, p. 236, 2024.

[24] J. Prakash, L. Murali, N. Manikandan, N. Nagaprasad, and K. Ramaswamy, "RETRACTED ARTICLE: A vehicular network based intelligent transport system for smart cities using machine learning algorithms," *Scientific reports*, vol. 14, no. 1, p. 468, 2024, doi: 10.1038/s41598-023-50906-7.

[25] D. S. Hemani and R. K. Dwivedi, "Designing blockchain based secure autonomous vehicular internet of things (IoT) architecture with efficient smart contracts," *International Journal of Information Technology*, pp. 1-17, 2024, doi: 10.1007/s41870-023-01712-x.

[26] K. S. Kaswan, V. Balu, A. Ojha, A. Sharma, D. Vekariya, and A. K. Marandi, "Deep learning algorithms and mechanisms in navigation for vehicular crowd management systems in real time for smart transportation," *Soft Computing*, pp. 1-12, 2023, doi: 10.1007/s00500-023-08398-0.

[27] R. Kumar and N. Agrawal, "A survey on software-defined vehicular networks (SDVNs): a security perspective," *The Journal of Supercomputing*, vol. 79, no. 8, pp. 8368-8400, 2023, doi: 10.1007/s11227-022-05008-y .

[28] E. A. Shams, A. Rizaner, and A. H. Ulusoy, "Flow-based intrusion detection system in vehicular ad hoc network using context-aware feature extraction," *Vehicular Communications*, vol. 41, p. 100585, 2023, doi: 10.1016/j.vehcom.2023.100585.

[29] H. Maghfiroh, M. R. Subeno, M. R. Darmawan, and R. Prihananto, "A Survey on Traction Motor and Its Prototyping Method for Electric Vehicle Application," *Journal of Electrical, Electronic, Information, and Communication Technology*, vol. 5, no. 1, pp. 21-26, 2023, doi: 10.20961/jeeict.5.1.71317.

[30] H. S. Dakheel, Z. B. Abdullah, and S. W. Shneen, "Simulation model of FLC-PID based speed control system for DC motor drive by using matlab," *AIP Conference Proceedings*, vol. 3002, no. 1, 2024, doi: 10.1063/5.0206580.

[31] C. Hermanu, H. Maghfiroh, H. P. Santoso, Z. Arifin, and C. Harsito, "Dual mode system of smart home based on internet of things, *Journal of Robotics and Control (JRC)*, vol. 3, no. 1, pp. 26-31, 2022, doi: 10.18196/jrc.v3i1.10961.

[32] Z. B. Abdullah, S. W. Shneen, and H. S. Dakheel, "Simulation model of PID controller for DC servo motor at variable and constant speed by using MATLAB," *Journal of Robotics and Control (JRC)*, vol. 4, no. 1, pp. 54-59, 2023, doi: 10.18196/jrc.v4i1.15866.

[33] H. Maghfiroh, C. Hermanu, M. H. Ibrahim, and M. Nizam, "Low Cost Charging Station for Electric Vehicle: Design and Prototyping," *2019 6th International Conference on Electric Vehicular Technology (ICEVT)*, pp. 20-24, 2019, doi: 10.1109/ICEVT48285.2019.8994011.

[34] S. W. Jeaeb, A. Z. Salman, Q. A. Jawad, and H. Shareef, "Advanced optimal by PSO-PI for DC motor," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 1, pp. 165-175, 2019, doi: 10.11591/ijeecs.v16.i1.pp165-175.

[35] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," *Vehicular Communications*, vol. 19, p. 100179, 2019, doi: 10.1016/j.vehcom.2019.100179.

[36] Y. A. Enaya, A. A. Karim, S. M. Saleh, and S. W. Shneen, "Adapting Wired TCP for Wireless Ad-hoc Networks Using Fuzzy Logic Control," *Journal Européen des Systèmes Automatisés*, vol. 57, no. 5, p. 1377, 2024, doi: 10.18280/jesa.570513.

[37] G. Yan and D. B. Rawat, "Vehicle-to-vehicle connectivity analysis for vehicular ad-hoc networks," *Ad Hoc Networks*, vol. 58, pp. 25-35, 2017, doi: 10.1016/j.adhoc.2016.11.017.

[38] Y. A. Enaya, A. A. Karim, M. Q. Sulttan, and S. W. Shneen, "Applying Proportional–Integral–Derivative Controllers on Wired Network TCP's Queue to Solve Its Incompatibility with the Wireless Ad-Hoc Network," *ITEGAM-JETIA*, vol. 10, no. 49, pp. 228-232, 2024, doi: 10.5935/jetia.v10i49.1346.

[39] M. A. Shamseldin, M. Araby, and S. El-khatib, "A Low-Cost High Performance Electric Vehicle Design Based on Variable Structure Fuzzy PID Control," *Journal of Robotics and Control (JRC)*, vol. 5, no. 6, pp. 1713-1721, 2024, doi: 10.18196/jrc.v5i6.22071.

[40] F. N. Abdullah, G. A. Aziz, and S. W. Shneen, "Simulation model of servo motor by using matlab." *Journal of Robotics and Control (JRC)*, vol. 3, no. 2, pp. 176-179, 2022, doi: 10.18196/jrc.v3i2.13959.

[41] N. T. Dang and Q. N. Duong, "Formation Control of Multiple Unmanned Aerial Vehicle Systems using Integral Reinforcement Learning," *Journal of Robotics and Control (JRC)*, vol. 5, no. 6, pp. 1736-1743, 2024, doi: 10.18196/jrc.v5i6.23505.

[42] H. S. Dakheel, Z. B. Abdullah, N. S. Jasim, and S. W. Shneen, "Simulation model of ANN and PID controller for direct current servo motor by using Matlab/Simulink," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 20, no. 4, pp. 922-932, 2022.

[43] A. A. Firdaus *et al*., "Application of sentiment analysis as an innovative approach to policy making: A review," *Journal of Robotics and Control (JRC)*, vol. 5, no. 6, pp. 1784-1798, 2024, doi: 10.18196/jrc.v5i6.22573iew/22573.

[44] A. L. Shuraiji and S. W. Shneen, "Fuzzy Logic Control and PID Controller for Brushless Permanent Magnetic Direct Current Motor: A Comparative Study," *Journal of Robotics and Control (JRC)*, vol. 3, no. 6, pp. 762-768, 2022, doi: 10.18196/jrc.v3i6.15974.

[45] F. Furizal, A. Ma'arif, and D. Rifaldi, "Application of machine learning in healthcare and medicine: A review," *Journal of Robotics and Control (JRC)*, vol. 4, no. 5, pp. 621-631, 2023, doi: 10.18196/jrc.v4i5.19640.

[46] N. P. Astuti, R. Ritzkal, A. H. Hendrawan, and B. A. Prakosa, "Vehicle security system using short message service (SMS) as a danger warning in motorcycle vehicles," *Journal of Robotics and Control (JRC)*, vol. 1, no. 6, pp. 224-228, 2020, doi: 10.18196/jrc.1642.

[47] S. W. Shneen, H. S. Dakheel, and Z. B. Abdullah, "Design and Implementation of No Load, Constant and Variable Load for DC Servo Motor," *Journal of Robotics and Control (JRC)*, vol. 4, no. 3, pp. 323-329, 2023, doi: 10.18196/jrc.v4i3.17387.

[48] A. A. Kurniawan *et al*., "Fuzzy logic method for making push notifications on monitoring system of IoT-based electric truck charging," *Bulletin of Electrical Engineering and Informatics*, vol. 14, no. 1, pp. 118-131, 2025, doi: 10.11591/eei.v14i1.7412.

[49] M. Husni, R. V. H. Ginardi, K. Gozali, R. Rahman, A. S. Indrawanti, and M. I. Senoaji, "Mobile security vehicle's based on internet of things," *Journal of Robotics and Control (JRC)*, vol. 2, no. 6, pp. 546-551, 2021, doi: 10.18196/jrc.26135.

[50] E. Gowthaman, V. Vinodhini, M. Y. Hussain, S. K. Dhinakaran, and T. Sabarinathan, "Speed control of permanent magnet brushless DC motor using hybrid fuzzy proportional plus integral plus derivative controller," *Energy Procedia*, vol. 117, pp. 1101-1108, 2017.

[51] F. Furizal *et al*., "Concerns of Ethical and Privacy in the Rapid Advancement of Artificial Intelligence: Directions, Challenges, and Solutions," *Journal of Robotics and Control (JRC)*, vol. 5, no. 6, pp. 2015-2026, 2024, doi: 10.18196/jrc.v5i6.24090.

[52] H. S. Dakheel, Z. B. Abdullah, and S. W. Shneen, "Advanced optimal GA-PID controller for BLDC motor," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 4, pp. 2077-2086, 2023, doi: 10.11591/eei.v12i4.4649.

[53] M. K. Khan and A. Quadri, "Augmenting Cybersecurity in Autonomous Vehicles: Innovative Recommendations for Aspiring Entrepreneurs," in *IEEE Consumer Electronics Magazine*, vol. 10, no. 3, pp. 111-116, 2021, doi: 10.1109/MCE.2020.3024513.

[54] A. J. Attiya, S. W. Shneen, B. A. Abbas, and Y. Wenyu, "Variable speed control using fuzzy-pid controller for two-phase hybrid stepping motor in robotic grinding," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 3, no. 1, pp. 102-118, 2016, doi: 10.11591/ijeecs.v3.i1.pp102-118.

[55] N. Wan and D. Wang, "A Novel Federated Learning Framework Based on Trust Evaluation in Internet of Vehicles," *Adhoc & Sensor Wireless Networks*, vol. 58, 2024, doi: 10.32908/ahswn.v58.10613.

[56] S. P. Devi and K. Dhanalakshmi, "MoDT: Interest Forwarding in Named Data Networking Based Vehicular Ad Hoc Networks by Predicting the Mobility Using Direction and Timer," *Ad Hoc & Sensor Wireless Networks*, vol. 58, no. 1-2, pp. 53-77, 2024, doi: 10.32908/ahswn.v58.8995.

[57] V. R. Azhaguramyaa and J. Janet, "Lightweight Health Data Security Protocol with Multi-Block Chaining Principles for Intelligent Wireless IoT-Fog Systems," *Adhoc & Sensor Wireless Networks*, vol. 57, 2023, doi: 10.32908/ahswn.v57.10629.

[58] D. A. J. Al-Khaffaf, "Integrated photonic secured reliable DWDM for 5G Xhaul at Ka band frequency," *Results in Optics*, vol. 13, p. 100558, 2023, doi: 10.1016/j.rio.2023.100558.

[59] D. A. J. Al-Khaffaf, "5G solution for existing indoor wireless radio access point of fronthaul mobile network," *AIP Conference Proceedings*, vol. 2290, pp. 40003-40003, 2020, doi: 10.1063/5.0027359.

[60] F. Farivar, M. Sayad Haghighi, A. Jolfaei, and S. Wen, "On the Security of Networked Control Systems in Smart Vehicle and Its Adaptive Cruise Control," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3824-3831, June 2021, doi: 10.1109/TITS.2021.3053406.