big data and cognitive computing

MDPI

Article

Confidential Intelligent Traffic Light Control System: Prevention of Unauthorized Traceability

Ahmad Audat [1,†], Maram Bani Younes [2,*,†], Marah Yahia [3,†] and Said Ghoul [4,†]

[1] Cybersecurity Department, Information Technology College, Amman Arab University, Amman 11953, Jordan; a.audat@aau.edu.jo
[2] Cybersecurity Department, Information Technology College, American University of Madaba, Madaba 11821, Jordan
[3] Software Engineering Department, Information Technology College, Jadara University, Irbid 21110, Jordan; m.sarireh@jadara.edu.jo
[4] Software Engineering Department, Information Technology College, Philadelphia University, Amman 19392, Jordan; sghoul@philadelphia.edu.jo
* Correspondence: mbani047@uottawa.ca
† These authors contributed equally to this work.

Abstract

Many research studies have designed intelligent traffic light scheduling algorithms. Some researchers rely on specialized sensors and hardware to gather real-time traffic data at signalized road intersections. Others benefit from artificial intelligence techniques and/or cloud computing technologies. The technology of vehicular networks has been widely used to gather the traffic characteristics of competing traffic flows at signalized road intersections. Intelligent traffic light controlling systems aim to fairly liberate competing traffic at signalized road intersections and eliminate traffic crises. These algorithms have been initially developed without focusing on the consequences of security threats or attacks. However, the accuracy of gathered traffic data at each road intersection affects its performance. Fake and corrupted packets highly affect the accuracy of the gathered traffic data. Thus, in this work, we aim to investigate the aspects of security and confidentiality of intelligent traffic light systems. The possible attacks on the confidentiality of intelligent traffic light systems are examined. Then, a confidential traffic light control system that protects the privacy of traveling vehicles and drivers is presented. The proposed algorithm mainly prevents unauthorized traceability and linkability attacks that threaten people's lives and violate their privacy. Finally, the proposed algorithm is evaluated through extensive experiments to verify its correctness and benefits compared to traditional insecure intelligent traffic light systems.

Keywords: smart traffic light; security; confidentiality; traceability; linkability

check for updates

Academic Editors: Nik Bessis, Qasem Abu Al-Haija, Ammar Odeh and Abdulaziz Alsulami

Received: 8 May 2025
Revised: 16 June 2025
Accepted: 18 June 2025
Published: 26 June 2025

Citation: Audat, A.; Younes, M.B.; Yahia, M.; Ghoul, S. Confidential Intelligent Traffic Light Control System: Prevention of Unauthorized Traceability. *Big Data Cogn. Comput.* **2025**, *9*, 169. https://doi.org/10.3390/bdcc9070169

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the rapid development of Internet-of-Things (IoT) technologies and increase in studies on smart cities, many systems have been developed to serve people and assist them in their daily activities. Intelligent transportation is one of the main fields that has been deeply investigated and developed [1,2]. Several protocols have been introduced to control autonomous vehicles on road networks [3,4]. Other protocols have been developed to assist drivers, especially in critical road scenarios [5–7]. Downtown road intersections introduce hazardous areas where conflicting traffic flows have to share them simultaneously. Traffic

lights have been used early on to control these intersections and allow conflicting traffic flows to safely and efficiently share these intersections [5,6,8].

Many studies have worked on designing intelligent algorithms to control traffic lights at road intersections [6,8]. Some of these studies have utilized special sensors and hardware to gather the traffic distribution around signalized road intersections [6,7]. Other studies have been designed based on artificial intelligence principles and historical data [9,10]. Cloud computing and vehicular network technologies have also been used to develop intelligent traffic light control systems based on real-time traffic data [4,11,12]. In general, these controlling systems aim to enhance the smoothness of traffic flow on the road network by reducing the wait delay time at signalized intersections and increasing the throughput of these intersections. The context of traversed traffic in terms of existing emergency or heavy vehicles has also been considered, and higher priorities have been assigned to these traffic flows [13–15].

The accuracy of gathered traffic data at each road intersection affects the performance of the traffic light control system. Fake and corrupted packets can deceive the system into producing a schedule for the located traffic light that serves the attackers and intruders around the intelligent traffic lights. Some research studies have considered security threats and possible attacks for intelligent traffic light control systems [16–19]. In this work, we mainly investigate the possible attacks on intelligent traffic light control systems. Focusing on confidentiality and privacy targets and their consequences. Vehicles and drivers should be able to hide their data, and secure protocols should be able to prevent traceability and linkability attacks in order to encourage them to cooperate with the intelligent traffic light controlling system. We mainly aim to detect threats to vehicles and drivers around intelligent traffic light control systems. Then, a confidential intelligent traffic light control system that tackles and prevents these possible attacks is introduced.

Furthermore, securing any system suffers extra complexity and requires more processing time [20]. The secure protocol should verify acceptable overhead in complexity and delay time, allowing reasonable system usability. This paper aims to investigate these overhead factors for the proposed protocol and confirm the acceptable overhead of securing the communication that does not prevent the main functionality of the algorithm.

The remainder of this paper is organized as follows: Section 2 investigates the previous studies that have developed intelligent traffic light control systems, illustrating their differences and similarities. Moreover, some popular mechanisms that aim to achieve confidential communication are also presented in that section. Section 3 studies the details of an intelligent traffic light system. It shows the possible input and output flows of a signalized road intersection and which flows can transfer through the intersection simultaneously. Section 4 investigates the possible attacks on the confidentiality of vehicles and drivers around these intelligent traffic lights, focusing on unauthorized traceability and linkability attacks. The confidential intelligent traffic light control system that intends to prevent these attacks is presented in Section 5. The proposed algorithm's performance is compared to the insecure algorithm in Section 6 to verify the correctness of the proposed algorithm and investigate its benefits and overhead. Finally, Section 7 concludes the entire paper.

2. Related Work

In this section, we first investigate some intelligent traffic light control systems. We illustrate the technology used, the main contribution, the road scenario handled, and the security threats that were considered. Then, a short review and comparative study of secure communication protocols developed for intelligent traffic management and mainly traffic light control systems is presented.

2.1. Intelligent Traffic Light Control Systems

Road intersections can be classified into two main categories over the road network: isolated and connected road intersections. At isolated road intersections the input traffic flows are not affected by other road intersections, and the output flows do not affect any other road intersection. On the other hand, connected intersections are located as part of an open or closed road network, where traffic flows of adjacent road intersections affect each other.

First, for isolated road intersections, the Intelligent Traffic Light Control (ITLC) algorithm [6] was designed. It identifies the sequence phases of each traffic light cycle and the time for each phase. This is according to the real-time traffic characteristics of the competing traffic flows [6]. Based on the traffic characteristics, the sequence of phases and the time for each phase are efficiently set [6]. This algorithm reduces the queuing delay time of vehicles at the signalized isolated road intersection. Moreover, it increases traffic fluency and the throughput of the road intersection. The traffic density, speed, and estimated travel time for each traffic flow within the ready area are calculated using the ECODE (i.e., efficient congestion detection) protocol [21]. Alharbi et al. [22] proposed a framework of smart traffic lights (STLs) to dynamically control and manage traffic lights. It determines the priority of passing through the intersection based on the level of traffic congestion, assessed by processing images taken by long-range digital cameras installed at the intersection.

Another study developed a traffic light scheduling algorithm for pedestrian-vehicle mixed-flow networks [23]. A macroscopic model that set an appropriate balance between pedestrians' needs and vehicle drivers' needs was employed to describe the traffic light scheduling problem in a scheduling framework. The main objective was to minimize the total network-wide delay time of vehicles and pedestrians within a given finite-time window, which is crucial to avoid traffic congestion in urban road networks.

Moreover, another dynamic traffic light scheduling algorithm (DTLS) [13] was designed for isolated road intersections. That algorithm helped emergency vehicles pass quickly through the signalized road intersection. It set the best green-phase time for each traffic flow based on the real-time traffic distribution at the signaled intersection. Using vehicle communication technology, the presence of an emergency vehicle heading to the traffic light was reported as soon as it appeared. The delivered emergency vehicle arrival report contained the type of emergency vehicle, its location, speed, and the target destination. Another dynamic traffic signal scheduling system based on an improved greedy algorithm was proposed in [24]. It introduced a reward function and a cost model to ensure fair scheduling plans. Moreover, an emergency module was integrated to prioritize special emergency vehicles, reducing their response time during emergencies.

Second, some research studies have considered open road network scenarios, where arterial streets are available with connected traffic lights, and assigned higher priorities to vehicles on these streets to pass through the intersection. The Arterial Traffic Light Controlling Algorithm (ATL) [6] is an algorithm that considers several existing traffic lights on a grid layout architecture. The ATL algorithm considers reservation notifications from nearby traffic lights on the arterial street while setting the schedule. In a traffic-signalized road network, a series of traffic lights installed on the road network coordinate with each other to achieve network-wide traffic management goals.

Moreover, another adaptive traffic light control system (ATLCS) was designed in [25] to schedule the competing traffic flows at signalized road intersections. That system also assigned higher priorities to vehicles leaving the intersection on the arterial road, aiming to synchronize the traffic light controllers located at the sequence of road intersections there. Magnetometers were used to sense and measure each road intersection's competing traffic flow characteristics. These sensors detected the presence of vehicles passing over them

by detecting the change in the Earth's magnetic field. Then, the readings of the existing magnetometers were delivered to the traffic light controller algorithm to be considered in the selected traffic light schedule. It did not consider any security threat. Recently, Jin [26] combined reinforcement learning and Markov decision to construct a signal control problem model for multiple intersections. Then, deep Q-learning networks were introduced for decision solving, and multi-head attention mechanisms and graph convolutional networks were further introduced for optimization and improvement. Moreover, a spatial lightweight model for multiple intersection adaptive graph convolution was proposed.

Third, for closed road network scenarios, a distributed architecture based on fog and the Efficient Dynamic Traffic Light Control Algorithm for Multiple traffic lights (EDTLCM) was proposed by Hossan et al. [11]. Intersections were constantly monitored, and dynamic traffic control decisions were based on real-time traffic information. Installed sensors at road intersections detected the number of incoming and outgoing vehicles. Then, the traffic characteristics were sent to the intersection's local gateway. Using these data, the local gateway calculated the waiting time, stopping time for vehicles, lane priorities, and state priorities. The local gateway transmitted the computed lane priorities to a nearby fog node. Each fog node was interconnected with neighboring fog nodes connected to a responsible cloud. The best possible solution was obtained by considering the local and neighboring information. Geographically distributed fog nodes were interconnected to cover the city, each connected to the cloud. The algorithm consisted of two main steps: detecting vehicles and a green light sequence, then determining the duration for each green phase. The simulation results showed that the suggested strategy had faster throughput, reduced waiting time, and used less fuel than alternatives [11]. Furthermore, Widied et al. [27] developed a smart simulator where traffic lights were constructed at intersections resembling those in large cities. The flow of vehicles through the grid was optimized by developing algorithms for how traffic lights changed their state. This maximized vehicle movement over the grid, and scheduling algorithms were developed to control how road traffic changed.

Table 1 summarizes the main characteristics of previously proposed intelligent traffic light control mechanisms, comparing the mechanisms used to gather the traffic characteristics, the technology used in the proposed algorithm, the main considerations of each algorithm, and the handled road scenario. These algorithms were mainly developed to schedule the phases of the traffic lights; none of them considered the security threats or their consequences. In the algorithms that utilize vehicular network technology [6,13], vehicles around the intelligent traffic lights communicate through beacon messages (i.e., regular messages announce each vehicle's location, speed, direction, target, etc.). The surrounding traffic receives the beacon messages, analyzes the gathered traffic data, and obtains general traffic characteristics for each traffic flow. These characteristics are reported to the intelligent traffic light and are to be considered in its schedule. Hackers, intruders, and criminals can easily capture these transmitted beacons and reported messages. They may use these messages to invade the vehicles' and drivers' privacy. Moreover, they can manipulate the transmitted messages to deceive these drivers and/or the intelligent traffic light and break the system's functionality.

Table 1. Intelligent traffic light control mechanisms.

Control Mechanism	Traffic Characteristics Gathering	Technology Used	Main Considerations	Handled Road Scenario	Considered Security Threat
ITLC [6]	Traffic speed, density, estimated traveling time, and the number of vehicles within the ready area for each traffic flow	Vehicular Ad Hoc Network (VANET)	Waiting delay time and throughput	Isolated road intersection	None
STL [22]	Level of Traffic Congestion	Images taken by long range digital camera	Waiting delay time and throughput	Isolated road intersection	None
Pedestrian–Vehicle [23]	Pedestrians' needs and vehicle drivers' needs	Vehicular Ad Hoc Network (VANET)	Total network-wise delay times of vehicles and pedestrians within a given finite-time window	Isolated road intersection	None
DTLS [13]	Traffic speed, density, estimated traveling time, and emergency vehicles existence	Vehicular Ad Hoc Network (VANET)	Traffic density and emergency vehicles	Isolated road intersection	None
Greedy [24]	Traffic speed, density, estimated traveling time, and emergency vehicles existence	Vehicular Ad Hoc Network (VANET), dataset for greedy algorithm	Traffic density and emergency vehicles	Isolated road intersection	None
ATL [6]	Traffic speed, density, estimated traveling time, and the number of vehicles within the ready area for each traffic flow.	Vehicular Ad Hoc Network (VANET)	Waiting delay time, throughput, and arrival platoons from neighboring intersections.	Open network or arterial street	None
ATLCS [25]	The presence of vehicles passing over the sensors	Vehicular Ad Hoc Network (VANET) and magnetometer sensors	Travel time is the number of occurrences of the "stop and go".	Downtown-area open-network or arterial street	None

Table 1. *Cont.*

Control Mechanism	Traffic Characteristics Gathering	Technology Used	Main Considerations	Handled Road Scenario	Considered Security Threat
AI Models [26]	Number of incoming and outgoing vehicles	Reinforcement learning and Markov decision, deep Q-learning networks, multi-head attention mechanisms, and graph convolutional networks	Average waiting time, fuel consumption, and throughput.	Open road network	None
EDTLCM [11]	Number of incoming and outgoing vehicles there	Fog computing and wireless sensors	Average waiting time, fuel consumption, and throughput.	Closed road network	None
Grid Optimizer [11]	Flow through the downtown grid	Optimization algorithms	Vehicle movement on the road network.	Closed road network	None

2.2. Secure Communication Protocols for Intelligent Traffic Management Systems

Several previous studies have considered the security requirements for intelligent traffic light control systems, especially in terms of providing secure connecting protocols [16–18,28,29]. A fog-based security framework for intelligent traffic light control systems (FSF-ITLCS) was presented by Khalid et al. [16]. That framework utilizes symmetric and asymmetric cryptography, hash functions, and digital signatures to ensure confidentiality, integrity, and credibility. Three main units are considered in the system: the Department of Motor Vehicles (DMV), roadside units (RSUs), and vehicles. The DMV is a fully trusted government agency. Its responsibility includes the installation of several roadside units (RSUs) equipped with computational capabilities and storage capacity within the designated region. The DMV is responsible for registering all automobiles in the system and issuing identification and signed tokens. RSUs function as governmental entities to provide services within a restricted range of 100 m. Their main responsibility is to transmit encrypted communications and certificates inside the designated surveillance area. Each vehicle in the system is equipped with an On-Board Unit (OBU) with communication and processing capabilities. Every car is officially registered with the Department of Motor Vehicles (DMV) and establishes direct communication with the accessible Roadside units (RSUs). The suggested FSF-ITLCS method uses a random seed problem given to each vehicle when it enters the monitored area after the calculated GeoLock value. Every vehicle is required to solve problems and adhere to protocols sent by the RSU. The suggested system effectively mitigated replay, denial of service, Sybil, and impersonation attacks [30–32].

Another secure traffic light management scheme in VANETs was proposed using fog computing technology [17]. This scheme was employed to fight against denial-of-service (DOS) attacks. It was developed based on the computational Diffie–Hellman (CDH) puzzle. The located traffic light generated a pool of CDH problems with varying hardness. The riddles were then encrypted and broadcast to surrounding automobiles using location-based encryption (LBE). Only vehicles inside the defined region could receive the riddles.

The receiver vehicles had to solve the riddle task within a certain time limit. After the riddle was solved, the vehicle generated evidence of solving it and sent it to the traffic light. The traffic light verified the legitimacy of the proof. The traffic light could execute a traffic schedule algorithm based on the proofs to alter the traffic light plans. A traffic signal under an enhanced scheme had to broadcast a single puzzle encrypted using an LBE technique to adjacent vehicles. The traffic light then had to execute extremely simple computations to validate the proofs. The hash collision puzzle served as the foundation for the enhanced approach. A traffic signal that used the newly designed puzzle only had to create one problem for all vehicles at each time slot. Thus, the calculation and communication overheads of the traffic signal were considerably minimized.

An Intelligent Traffic Management System (ITMS) based on an existing VANET and the Internet of Vehicles (IoV) that is appropriate for future traffic systems and smart cities was recently proposed [18]. The architecture of the proposed ITMS and Smart Traffic Signal (STS) controller was presented. The ITMS first needed communication technologies between the traveling vehicles and the infrastructure deployed along the road using VANETs. The infrastructure was a network of roadside units (RSUs). Moreover, a Global Navigation Satellite System (GNSS) was used to determine the vehicle's position, direction, and speed. The Smart Traffic Light (STS) was added as an On-Board Unit (OBU) that worked with the ITMS system to provide all required services. Security and anti-tampering units provided the necessary level of vehicle security and privacy. It held the vehicle's digital certificate issued by the transportation agency or manufacturer. It also had a set of anonymous certificates for communicating with other cars to preserve the driver's privacy and avoid vehicle monitoring. This unit safeguarded communications between automobiles and other units, such as traffic signals. The RSUs regularly sent certificates of trustworthy intelligent traffic lights to guarantee that cars always talked with real traffic signals [18]. Finally, another study proposed [19] a security and privacy-based access control (SPBAC) mechanism for the Internet of Connected Vehicles. This gave security administrators access to information as well as permissions and roles. Vehicles connected via an On-Board Unit (OBU), and the SPBAC paradigm enabled safe, confidential, and efficient vehicle communication.

Furthermore, Y. Feng [33] discusses the vulnerability of traffic control systems to cyberattacks involving falsified data. The author demonstrates how an attacker can use false information to manipulate traffic flow, leading to congestion and potentially causing accidents. The study suggests several solutions to mitigate the risks of cyberattacks on traffic control systems, including improved authentication methods, real-time monitoring and analysis of traffic data, and redundancy measures to prevent single points of failure. Additionally, that work suggests that traffic control systems should be designed with security in mind from the outset rather than being treated as an afterthought. Table 2 summarizes the main technologies used to secure intelligent traffic light control systems over the road network. The security tools used and the attacks handled are clearly illustrated in this table.

As we can infer, several secure traffic light scheduling algorithms have been proposed in the literature. However, none of the earlier studies have specifically considered the traceability and linkability issues of vehicles and drivers around intelligent traffic lights. These problems can be crucial in scenarios that mainly rely on VANET technology to gather real-time traffic characteristics of competing traffic flows. This motivated us in this study to introduce a confidential traffic light control system that mainly aimed to protect the privacy of vehicles and avoid unauthorized linkability between vehicles and their drivers.

Table 2. Comparison of technologies for securing intelligent traffic light control systems.

Secure Mechanism	Technology Used	Security Tool	Handled Attacks
FSF-ITLCS, Khalid, T. [16]	Fog computing	Utilizes symmetric, asymmetric cryptography, hash function, and digital signature to ensure confidentiality, integrity, and credibility.	Replay attacks, denial of service, Sybil, and impersonation attacks.
STLMS, Liu, J. [17]	Fog computing	Computational Diffie–Hellman (CDH) puzzle.	Denial of service
ITMS, Els, M. [18]	Internet of Vehicles (IoV) and VANETs	Digital certificates, security and anti-tampering units and a set of anonymous certificates	Privacy and tampering attacks
SPBAC, Habib, M. [19]	Internet of Connected Vehicles (IoCV)	A Security and Privacy-Based Access Control (SPBAC) model for the Internet of Connected Vehicles.	Unauthorized access and data theft.
VTCS, Feng, Y. [33]	Use advanced data analysis methods	Implement a comprehensive security framework	A cyberattack with falsified data

3. Traffic Light Control System

Traffic lights serve as essential traffic management tools. This is particularly true at intersections where multiple roads meet, and vehicles compete to traverse the shared intersection from different flows. Traditionally, traffic lights control the competing traffic flows using predetermined times of green, yellow, and red signals. This allows one or more non-conflicting traffic flows to move while others wait [34,35]. Traffic light systems are introduced to allow multiple open lanes for the simultaneous movement of vehicles in different directions through the road intersection. Provided that all the allowed traffic flows do not conflict with each other. This strategy optimizes traffic flow and minimizes congestion, resulting in smoother and more efficient traffic movements [36,37]. However, advancements in traffic engineering have introduced a more sophisticated approach to reducing traffic congestion and waiting delay times at signalized road intersections by considering an adaptive duration for each phase of the traffic light according to the traffic characteristics of the competing traffic flows [38,39].

Traffic engineers carefully analyze the traffic patterns at each intersection, identifying non-conflicting traffic flows that can be safely accommodated simultaneously. By coordinating the timings of the traffic lights and assigning specific lanes to different movements, vehicles can navigate through the intersection without having to wait for a long time, significantly reducing travel times and enhancing overall transportation efficiency [11]. Advanced technologies, such as traffic sensors and adaptive signal control systems, enable real-time adjustments to traffic light timings based on real-time traffic conditions. These systems use data from traffic cameras and sensors to monitor the flow of vehicles and adjust the signal timings accordingly, ensuring optimal traffic flow at all times [25,40]. For example, at a four-leg road intersection, if there are separate lanes for left turns, right turns, and straight movements, then the traffic lights should be programmed to allow vehicles in all these lanes to move simultaneously when these traffic flows have no conflict. This can be

achieved by adjusting the signal timings and introducing dedicated turn phases. Figure 1 illustrates the scenarios in which more than one traffic flow can be opened without conflict.

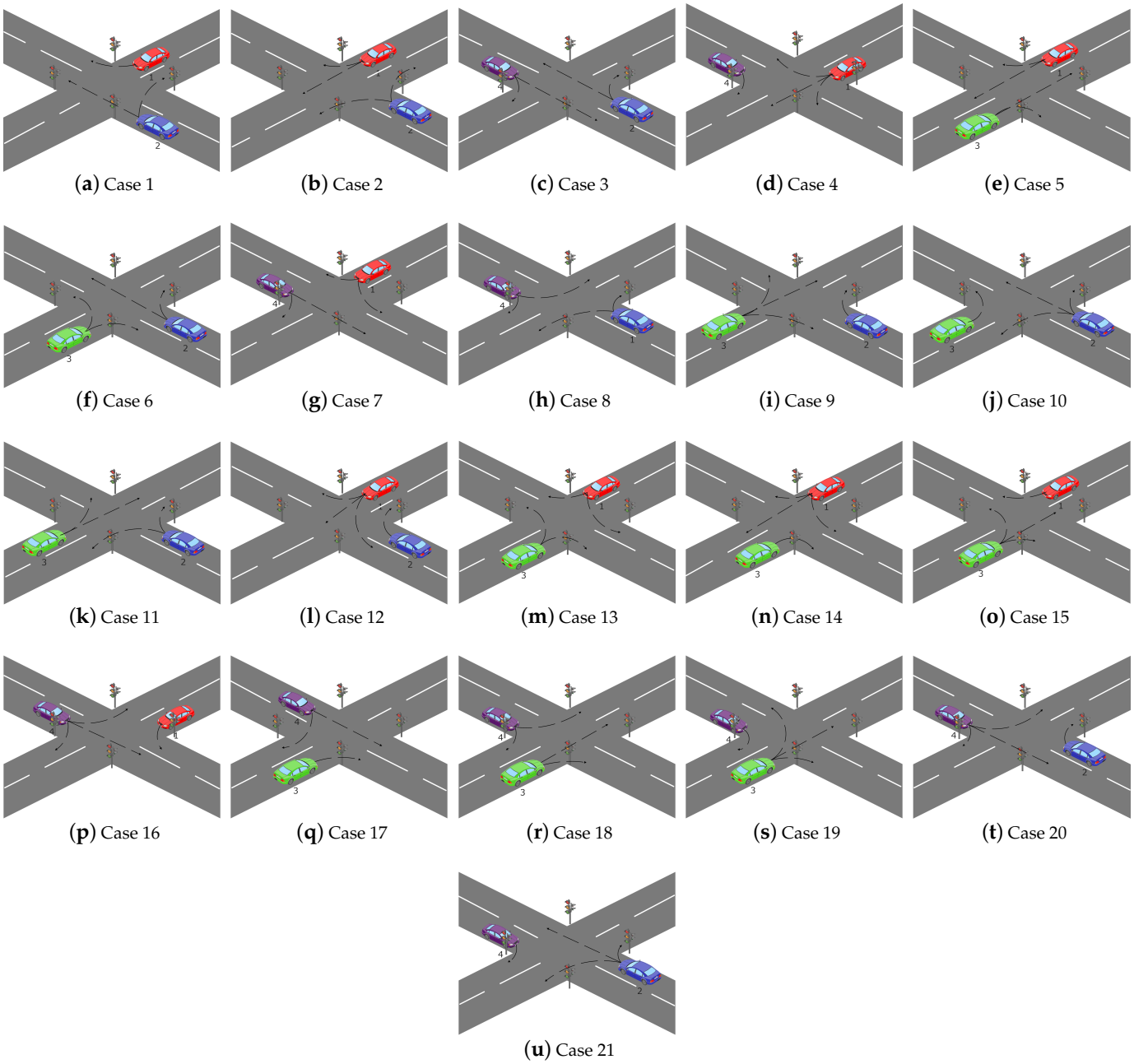


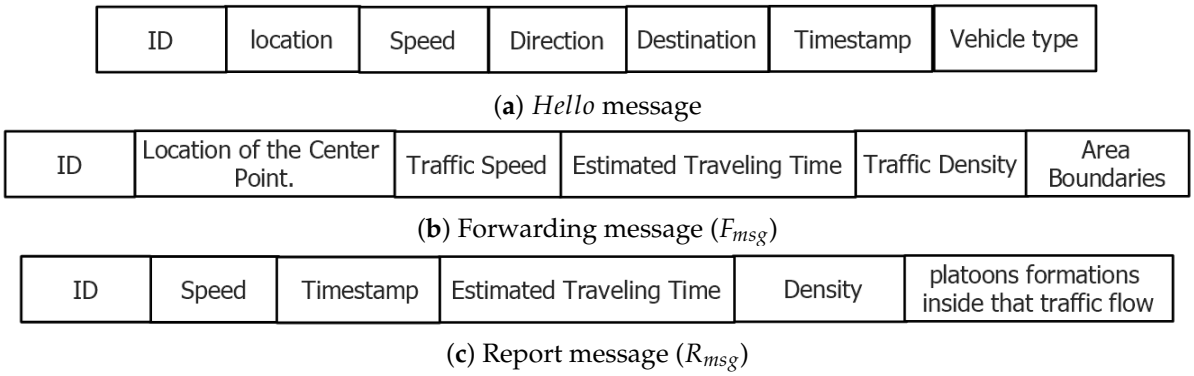
Figure 1. Possible cases of traffic flows that can traverse the intersection simultaneously.

For example, case (1) in Figure 1a shows how the signal activation of the two different lanes proceeds together when the red and blue cars remain stationary. Simultaneously activating both signals creates a smooth road for every car, eliminating any possibility of collisions in their respective directions. The red vehicle smoothly traverses the signal within a single lane, while the blue vehicle navigates the intersection with equal finesse, spanning its course across two distinct lanes.

Recently, vehicles on the road network have been equipped with several intelligent devices and tools. These types of equipment aim to enhance the intelligence of vehicles and allow them to make smart decisions during their trips. Among the several intelligent and recently used technologies in smart transportation is the technology of vehicular networks,

which allows vehicles to communicate on road networks. It mainly requires equipping vehicles with wireless transceivers to send and receive messages. Smart traffic lights are installed on the road network at intersections to control the competing traffic flows. Adaptive systems that consider real-time traffic characteristics are used to schedule the sequence of phases for these traffic lights. Thus, real-time traffic characteristics are required to set the schedules of these traffic lights. Vehicular network technology can evaluate the characteristics of each traffic flow.

Figure 2 illustrates the main components of the three main required messages in smart adaptive traffic light scheduling algorithms. As vehicles move, they periodically broadcast "*Hello*" messages. These messages transfer the basic data of each vehicle to its surrounding vehicles and infrastructures (i.e., roadside units). The basic data mainly includes the vehicle's identity (i.e., plate number), location, speed, direction, destination, and other parameters such as timestamp and vehicle type. Figure 2a illustrates the main fields of the *Hello* message. Upon receiving several "*Hello*" messages from neighboring vehicles, each vehicle can compute its surrounding area's traffic speed and density (i.e., traffic characteristics inside its transmission range). Then, forwarding the traffic characteristics in a multi-hop fashion through different transmission ranges helps the vehicles generate a more general traffic evaluation of an extended area of interest that may cover the entire road scenario. Forwarding messages (F_{msg}'s) are transferred by elected vehicles between different transmission ranges. F_{msg} contains mainly the identity of the forwarding vehicle, the boundaries of the considered area, the traffic speed, traffic density, estimated traveling time, and other parameters such as timestamp and location of the center point of the considered area of interest. Figure 2b illustrates the main fields of the F_{msg} message. Upon receiving F_{msg}'s, the boundaries of the evaluated area are extended, and the considered traffic characteristics at each considered vehicle are updated accordingly.



(**a**) *Hello* message

(**b**) Forwarding message (F_{msg})

(**c**) Report message (R_{msg})

Figure 2. The contents of regular messages to control traffic at road intersections.

Finally, for each road segment, the traffic characteristics are reported directly to the located traffic light. A report message (R_{msg}) is delivered from another elected vehicle (i.e., the closest vehicle to the traffic light) to the located traffic light. The latter message mainly contains the identity of the sender vehicles, the traffic characteristics of the contained traffic flow (i.e., traffic speed, traffic density, estimated arrival time, etc.), and other parameters such as timestamps and platoon formations inside that traffic flow. Figure 2c illustrates the main fields of the R_{msg} message. Upon receiving R_{msg}'s from all competing traffic flows, the installed traffic light can efficiently set the schedule of its phases.

Based on these messages and the communications among traveling vehicles and installed traffic lights, the data regarding the competing traffic flows are gathered inside the traffic light. The intelligent traffic light sets the sequence of phases of its cycles accordingly. This is considering the traffic distribution on the road network and the traffic context.

Some innovative traffic light scheduling and lane management strategies aim to create a harmonious traffic ecosystem. By efficiently organizing traffic flows and reducing congestion, these approaches improve safety, reduce greenhouse gas emissions, and enhance the overall commuting experience for road users [41]. Integrating modern traffic management techniques to control traffic light systems benefits road users and contributes to building more innovative and more sustainable urban environments [42].

4. Possible Attacks at Intelligent Traffic Light Systems

Intelligent traffic light control systems are vulnerable to several attacks that threaten the safety and privacy of traveling vehicles on the road network and their drivers. In this section, we investigate the possible attacks on the confidentiality of traveling vehicles and their drivers. This includes the threat of revealing the personal data of traveling vehicles and drivers [43–45]. In this work, we focused on unauthorized traceability and linkability threats.

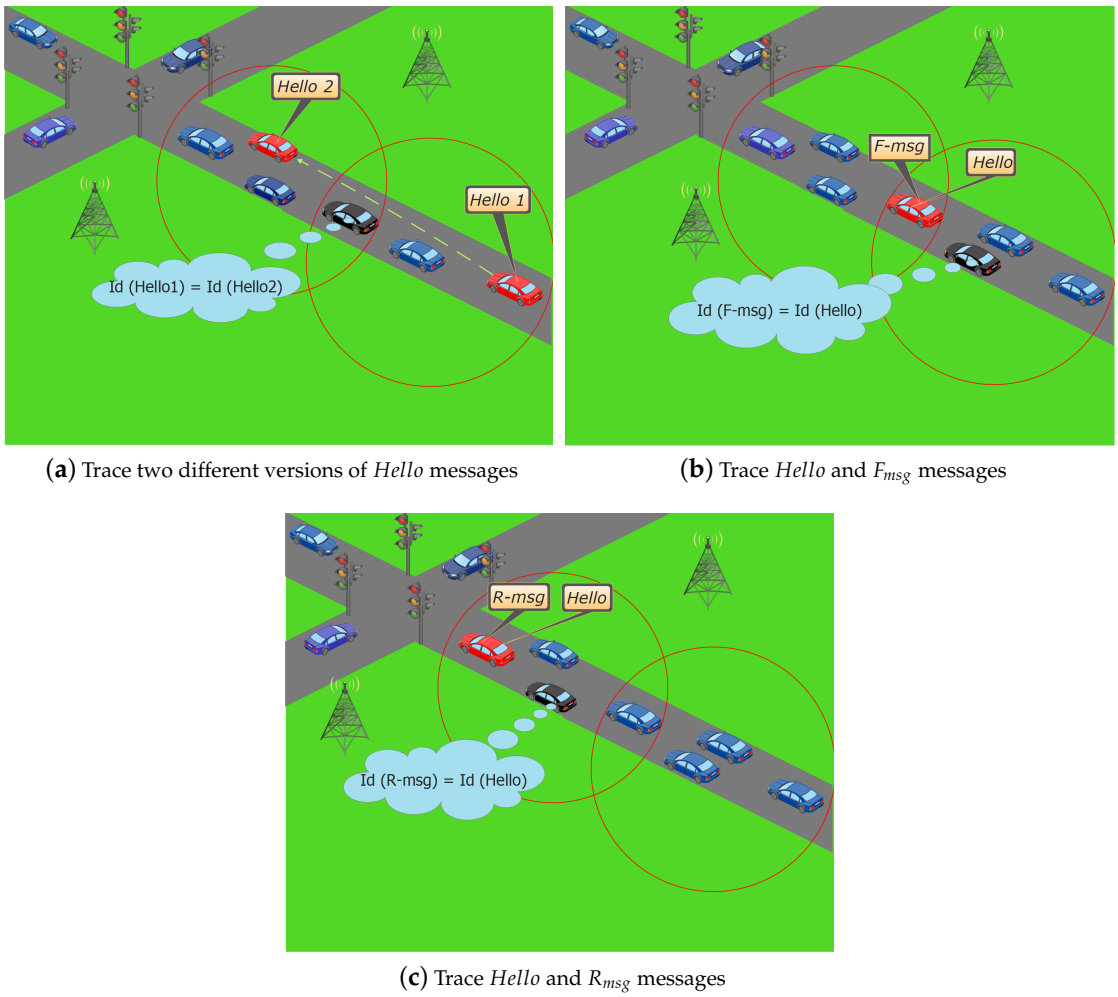
Unauthorized Traceability Attack

The traffic authority over each country should be able to trace vehicles over the road networks and link the identity of each vehicle to its driver and/or owner. Traceability defines the ability to trace certain vehicles' actions over the network. This includes their broadcast messages, requesting services, or reporting cases. This helps to trace their locations and identities, which should be helpful for finding intruders or criminals. On the other hand, linkability refers to the case where a tracing entity can link a vehicle's identity to its driver/owner. This is introduced to localize people and trace their information over the road network.

However, any unauthorized entity that tries to trace, stalk, or link vehicles and drivers' identities is classified as an intruder or criminal entity. Advanced communication technologies, such as vehicular network technology, are used in the smart environment. Then, traceability and linkability attacks are transferred into this cyberenvironment and connected to the transferred messages. Authorized traceability and linkability should be allowed, while unauthorized traceability and linkability should be completely prevented.

Here, we clearly illustrate the possible traceability attacks on the traffic evaluation phase that proceeds to the traffic light scheduling phase. As discussed in the previous section, three main messages are transferred during the traffic evaluation phase for each traffic flow (i.e., $Hello$, F_{msg}, R_{msg}). Sending and receiving these messages are vehicles' actions in the cyberenvironment (i.e., vehicular network communication). Thus, a traceability attack on this system includes mainly the intruder's ability to trace each vehicle's actions while participating in the traffic evaluation protocol. Figure 3 graphically illustrates three main scenarios of possible traceability attacks in the intelligent traffic light control system.

In Figure 3, the circles illustrate different considered areas over the same traffic flow. The boundaries of each area are set the same as the transmission range of traveling vehicles. However, the overlap between the two areas is required to allow vehicles located there to communicate with vehicles in both areas. Thus, these vehicles are responsible for forwarding the traffic characteristics of each area toward vehicles located in the neighboring area to extend the boundaries of the evaluated area of interest to consider the entire traffic flow.



(**a**) Trace two different versions of *Hello* messages

(**b**) Trace *Hello* and F_{msg} messages

(**c**) Trace *Hello* and R_{msg} messages

Figure 3. The scenarios of possible traceability attacks.

In Figure 3a, the attacker appears as a black vehicle on the road. It was able to trace the actions of the red vehicle (i.e., the victim's vehicle) by tracing two different versions of the *Hello* message broadcast by that vehicle at two different times. It was determined that the two *Hello* messages were sent by the same vehicle by retrieving the vehicle identity field in these messages. Figure 3b illustrates another traceability scenario where the attacker can trace two different messages sent by the same victim vehicle (i.e., *Hello* and F_{msg}). Another scenario appears in Figure 3c, where the attacker can trace *Hello* and R_{msg} sent by the same vehicle. Being vulnerable to losing privacy and being traceable by intruders and criminals discourages vehicles from cooperating with these protocols and intelligent systems. Moreover, criminals and mischievous individuals may take advantage of these scenarios to harm drivers and invade their privacy.

5. Proposed Confidential Intelligent Traffic Light Control System

In this section, we introduce a Confidential Intelligent Traffic Light Control System (CITLCS). This system incorporates attribute-based encryption to ensure privacy and security in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Attribute-based encryption (ABE) is a cryptographic technique that uses a set of public attributes as the basis for fine-grained resource protection [46]. The primary goal of the CITLCS is to limit the exposure of information to unauthorized entities and preserve anonymity within the network. Moreover, it aims to prevent all unauthorized traceability and linkability of vehicles' identities to enhance the safety conditions and privacy of vehicles

and their drivers. Figure 4 systematically illustrates the message encryption process in the proposed confidential protocol. The main steps of the CITLCS are summarized in the following four points.

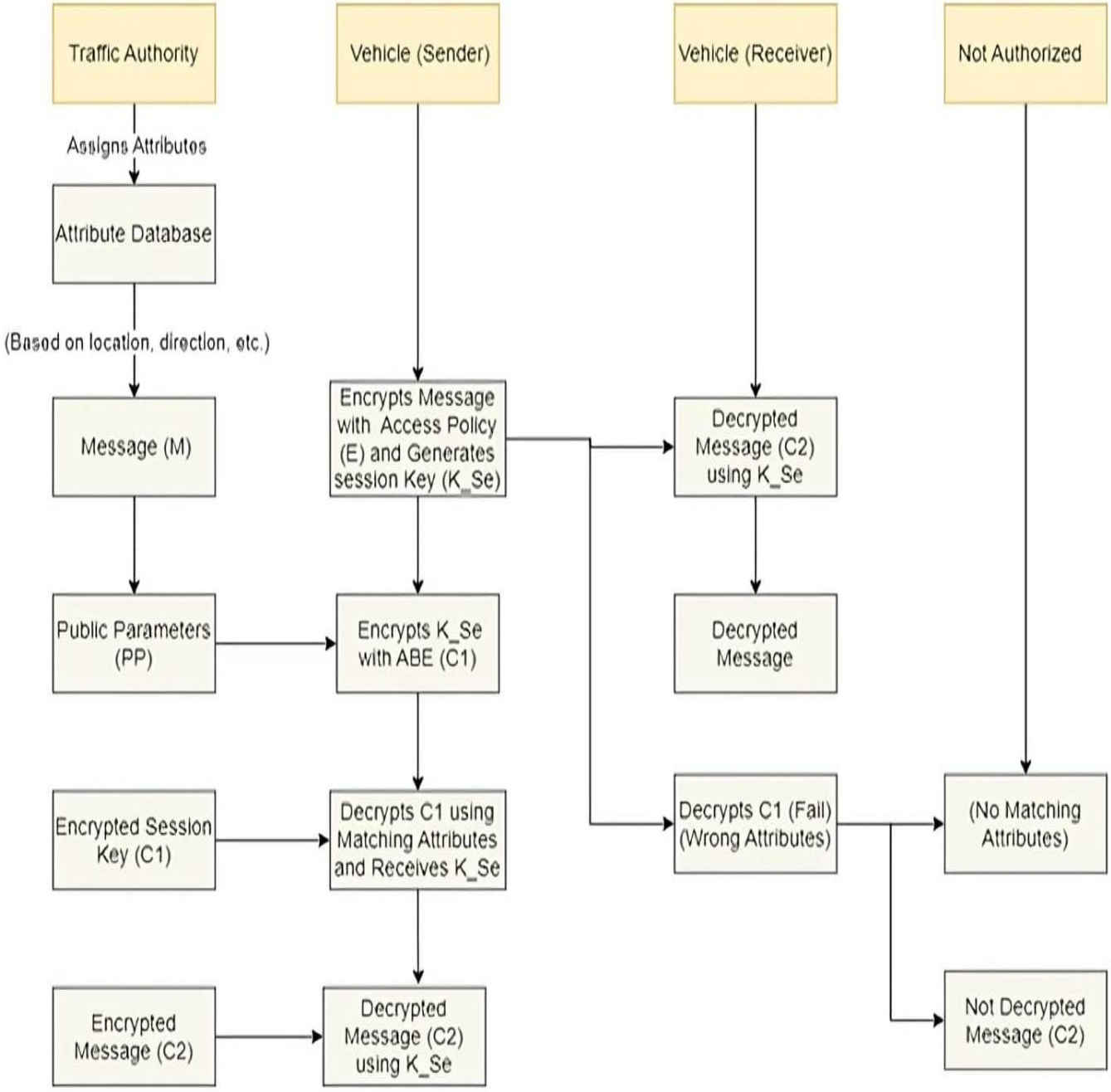


Figure 4. Message encryption process for authorized vehicles in CITLCS.

Step 1: Attribute Assignment

The traffic authority, controlling the competing traffic flows at road intersections, extracts the attributes of each vehicle based on its characteristics and role within the road network. The vehicle's attributes are selected mainly based on its location on the street relative to the location of the traffic light. The main goal is to monitor and control vehicle communications around the traffic light, without revealing the privacy of the vehicle or

driver. Each vehicle is defined according to its type, speed, location on the street, and ability to communicate with vehicles around the traffic light.

The main considered attributes of each vehicle could be listed as follows:

- $Distance_from_Traffic_Light$: indicates the distance between the vehicle and the traffic light. This attribute needs sensors or Global Positioning System (GPS) tools to measure it accordingly.
- $Direction_from_Traffic_Light$: indicates the direction of each vehicle concerning the traffic light. It determines whether the vehicle is moving toward or away from the traffic light: "Toward" or "Away" options. This attribute is determined based on the vehicle's position and movements on the road.
- $Lane_Position$: denotes the specific lane in which the vehicle is situated. It could be specified as *leftmost lane*, *middle lane*, or *rightmost lane*. This attribute helps determine the vehicle's lateral position concerning the traffic light.
- $Vehicle_Type$: The vehicle category may be identified internally based on its registration information. It can be categorized as a regular vehicle, truck, motorcycle, etc.
- $Speed$: The vehicle's speed may be determined by onboard sensors such as radars. The speed characteristic is crucial for managing traffic flow and altering the timings of traffic lights depending on the speed at which vehicles are approaching.

Vehicles can intelligently set the attributes for the encryption process while transmitting messages. However, the accurately assigned values of these attributes are required to proceed with the attribute-based encryption process. For example, a vehicle located close (i.e., 10 m) to the traffic light in the rightmost lane may encode its message using the following attributes:

"$Distance_from_Traffic_Light = 10m$",
"$Direction_from_Traffic_Light = Toward$",
"$Lane_Position = RightmostLane$",
"$Vehicle_Type = Regular$",
"$Speed = 50\,k/h$".

The traffic management system guarantees the precise identification and allocation of these characteristics. Additionally, it guarantees that the characteristic values are uniform and dependable for efficient traffic control and communication. Subsequently, traveling vehicles use these attributes while encrypting their messages. This ensures secure communication among traveling vehicles around the traffic light. Utilizing the attribute-based cryptographic algorithm, only vehicles that announce accurate attributes can decrypt the encrypted data correctly. This enables effective and protected communication among vehicles around the signalized road junction and between traveling vehicles and the smartly located traffic light.

Step 2: Key generation and setup procedure

This includes the development of public and private keys, followed by distributing these keys to the appropriate entities (i.e., vehicles and traffic lights) within the system.

- Key Generation: The key generation procedure, often referred to as the Key Authority (KA), is performed by a reliable and authoritative entity. In a real road scenario, this can be accomplished by roadside units (RSUs) that are connected directly to the traffic authority. The Key Authority (KA) generates the master secret key (MSK) and the appropriate public parameters (PPs) required for the attribute-based encryption (ABE) scheme. The MSK is highly sensitive information that must be securely maintained and used to create private keys associated with certain properties. For the key creation process, the NIST P-256 elliptic curve [47] is a viable choice for pairing operations.

This option facilitates the efficient pairing processes for implementing attribute-based encryption (ABE).

- Attribute-Based Encryption Setup: The public parameters (PPs) produced by the key authority (KA) are openly disseminated and accessible to vehicles and infrastructures (i.e., smart traffic lights) in the system. Including these public parameters (PPs) is crucial for executing the ABE method's encryption and decryption procedures. This includes the details of the privacy policy, the selected cryptographic algorithms, system configurations, and other essential information required to ensure safe encryption and decryption.
- Private Key Generation: After the generation of the master secret key (MSK) by the KA, each vehicle proceeds to produce a private key that corresponds to its specified attributes. Each vehicle obtains a unique private key that corresponds to the characteristics granted to it during the attribute assignment process. The KA announces the MSK and the qualities to produce a unique private key for each vehicle according to their assigned attributes.
- Private Key Distribution: The KA generates private keys for each vehicle and securely distributes them to the respective vehicles. The distribution of private keys must provide secrecy and integrity to prevent unauthorized access to the keys. For the distribution of private keys, KA uses secure communication methods that guarantee the secrecy and integrity of the key transfer. The channels are created between KA and vehicles in motion, enabling the safe transfer of private keys. This strategy was selected based on its efficacy in thwarting unauthorized access to the keys. It is important to emphasize that private keys are only given to vehicles and entities with legitimate attributes issued by the traffic management system. This guarantees that only approved vehicles can use encrypted messages to transmit and exchange.
- Updating Keys: In a dynamic traffic environment, the attributes of vehicles may change over time (e.g., as vehicles move closer or farther from the traffic light). The system should have mechanisms to update or revoke private keys to accommodate attribute updates. The key authority securely manages key updates and revocations. Updating the keys regularly based on the attributes of the vehicles is the main feature that prevents unauthorized traceability and linkability.

Step 3: Message Encryption

When a vehicle sends a message, it first determines the intended recipients and defines the access policy of its recipients. The access policy specifies the attributes these recipients must possess to decrypt and access the message successfully. For example, the sender vehicle might define an access policy as follows:

"$Direction = Northbound$",
"$Location = Main_Street$".

Then, it retrieves the public parameters (PPs) generated by the KA during the setup process. The public parameters include the necessary information for the ABE scheme. Additionally, the sender vehicle shares the access policy (e.g., "$Direction = Northbound$" and "$Location = Main_Street$") with the intended recipients of its message (M). It utilizes the shared access policy and public parameters received from the key authority for encrypting the message (M). The encryption process comprises the following steps:

1. Access Policy Encoding: Converts the access policy into a mathematical form appropriate for attribute-based encryption (ABE) operations. The access policy comprises logical expressions that are determined by the characteristics given to the receivers.
2. Random Session Key Generation: Produces a random session key (K_{Se}). This key is used to encrypt the actual message "M".

3. Attribute-Based Encryption: Performs the attribute-based encryption on the session key (K_{Se}) using the encoded access policy and the public parameters. This produces the ciphertext representing the encrypted session key. We denote this encrypted value by (C1), as illustrated in Equation (1):

$$C1 = ABE(K_{Se}) \tag{1}$$

4. Symmetric Encryption: Symmetrically encrypts the actual message "M" using the session key "K_{Se}", generating another ciphertext (C2), as illustrated in Equation (2):

$$C2 = K_{Se}(M) \tag{2}$$

The new messages for the proposed secure protocol are illustrated in Figure 5, with modifications to their contents. Figure 5a illustrates the new fields of the *Hello* message. Figure 5b illustrates the fields of the new F_{msg} message, and Figure 5c illustrates the fields of the new R_{msg} message. As we can infer from the figures, the new versions of $Hello_{Message}$, F_{msg}, and R_{msg} contain the same fields and contents as the messages used in the original insecure protocol. However, the contents of the new message are encrypted, and extra fields are appended to the new messages. These extra fields combine the ciphertexts generated during the encryption process (i.e., C1 and C2) and the required access policy information ($Policy_info$). The $Policy_Info$ part of the encrypted message contains information about the access policy used during the encryption process. It specifies the attributes that the recipients must possess to decrypt the message successfully. The $Policy_Info$ may be encoded in a format that can be easily processed by the recipient vehicles.

Encrypted Message $(C1, C2, Policy_info)$						
ID	Location	Speed	Direction	Destination	Timestamp	Vehicle Type

(**a**) New *Hello* message

Encrypted Message ${C1, C2, Policy_Info}$					
ID	Location of the Center Point	Traffic Speed	Estimated Traveling Time	Traffic Density	Area Boundaries

(**b**) New forwarding message (F_{msg})

Encrypted Message ${C1, C2, Policy_Info}$					
ID	Speed	Timestamp	Estimated Traveling Time	Density	Platoon formations inside that traffic flow

(**c**) New report message (R_{msg})

Figure 5. Traffic control messages of the new proposed secure protocol.

Step 4: Message Transmission

Upon receiving the encrypted message at any vehicle in the network, based on the type of the message (i.e., *Hello*, F_{msg}, or R_{msg}), the vehicle takes the most suitable action

and assumes the receiver role on the road network. The decryption process of the received messages is performed at the receiver vehicle. These recipients employ their private keys, generated according to their designated attributes, to decrypt the ciphertext C1.

Successful decryption occurs if their attributes align with the access policy, enabling them to recover the session key K_{Se}. With the obtained K_{Se}, they can then decrypt the symmetrically encrypted message C2, revealing the original message M. The direct involvement of vehicles in the encryption process within attribute-based encryption (ABE) guarantees accurate encryption execution based on the specified access policy. This approach was mainly developed to prevent unauthorized traceability and linkability of vehicles' locations and their successive actions on the road network, as discussed earlier. Since the vehicles change their locations and speeds on the network, the PP used to encrypt the K_{Se} is changed accordingly.

Moreover, the system randomly and regularly changes K_{Se}. Thus, intruder nodes can still illegally capture the encrypted messages of vehicles on the network. Moreover, they can parse and process these messages. However, they cannot retrieve the vehicle's original identity, trace its locations, or link two different messages or the identity of their senders if they have been sent by that same vehicle.

6. Performance Evaluation and Result Discussion

In this section, we aim to evaluate the performance of the proposed protocol. First, we tested the correctness of the proposed protocol and its ability to prevent traceability attacks in several scenarios around the traffic light. Then, we investigated the efficiency of this protocol in terms of the extra time and throughput required to secure the communications. The proposed protocol did not affect the performance of the traffic light because it did not consider the communication between vehicles and the traffic light or the sequence of phases at each traffic light.

The simulated experiments were conducted on an isolated traffic light system with eight competing traffic flows. NS-2 [48] was used to simulate traveling intelligent vehicles, and SUMO [49,50] generated their mobility in these experiments. The original intelligent traffic light control system cite C11 and the new secured version (i.e., proposed protocol) were implemented and tested. Their performance was compared for different scenarios. Table 3 illustrates the main parameters in the simulated experiments.

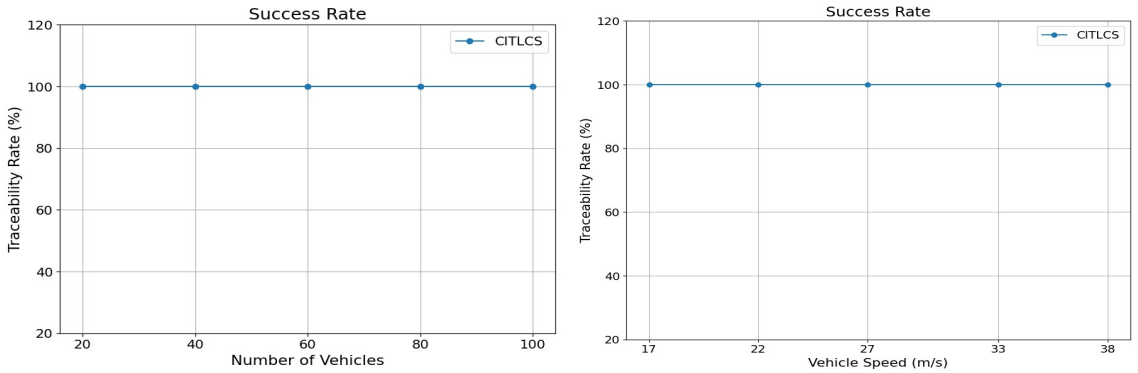
Table 3. Simulation parameters.

Parameter	Value
MAC type	IEEE802.11P
Transmission range (m)	200
Vehicle's speed (m/s)	17, 22, 27, 33, 38
Simulation area (m^2)	1000 m × 1000 m
Number of vehicles	20, 40, 60, 80, 100
Simulation time	10,000

6.1. Preventing Traceability Attacks

The ability of the proposed Confidential Intelligent Traffic Light Control System (CITLCS) to prevent traceability attacks is an essential factor in assessing the system's correctness. The number of vehicles around the signalized road intersection and the average speed of traveling vehicles are the main factors that may affect the correctness of the proposed system. Thus, several experiments were conducted to test the proposed system's ability to prevent traceability attacks on participating vehicles.

Figure 6 graphically illustrates the ability of the proposed system to prevent traceability attacks on vehicles around intelligent traffic lights. As we can infer from Figure 6a, the proposed system successfully prevented 100% of the attacks for different numbers of vehicles. This confirmed the scalability attribute of the system, which can handle small and large numbers of vehicles. Figure 6b also shows that the proposed system could detect 100% of the traceability attacks for different traveling speeds of vehicles. This confirmed the adaptability feature of the system.



(**a**) Preventing traceability for different numbers of vehicles (**b**) Preventing traceability for different traffic speeds

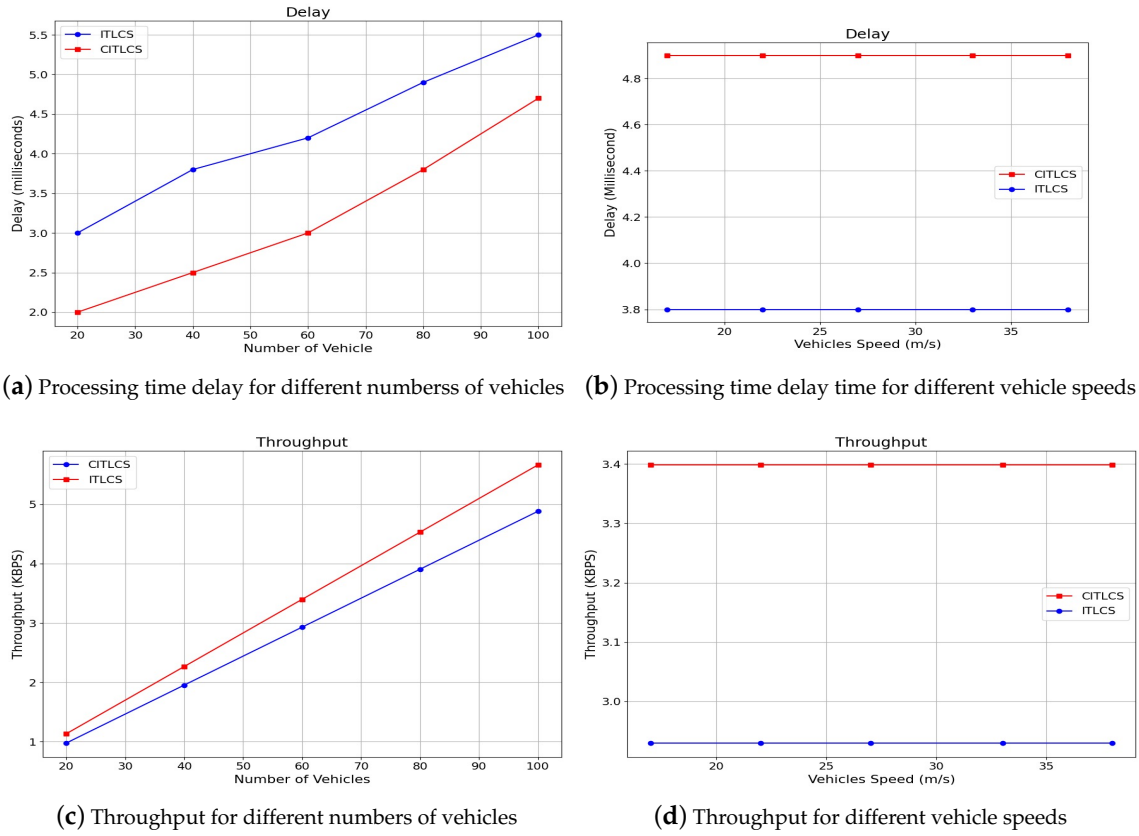
Figure 6. Preventing traceability attacks.

6.2. Efficiency of CITLCS

Security and privacy are valuable targets that are good to have in any system. However, the security overhead is summarized mainly by the required delay time to encrypt and decrypt messages, besides increasing the size of the transmitted message, which consumes more network bandwidth (i.e., higher throughput). Here, we measured these metrics to evaluate the efficiency of the proposed system (i.e., CITLCS) compared to the insecure version of the intelligent traffic light control system (i.e., ITLCS) [6]. Figure 7 illustrates the efficiency parameters of the ITLCS.

First, measuring the processing time delay for different numbers of vehicles and for different speed times is a key factor in evaluating the responsiveness of the CITLCS compared to the ITLCS. It mainly represents the required time for a message or command to traverse the system between a source and destination (i.e., V2V or V2I). The delay analysis encompassed scenarios with varying loads and network conditions to provide insights into the impact of security protocols on communication speed. Figure 7a illustrates the processing time comparison between the confidential, secure ITLC and the insecure version of ITLC for different numbers of vehicles. As we can infer from the Figure, the secure version required more than 30% extra processing time. This is due to the encryption and description processes. More overhead in terms of delay appeared for a higher number of vehicles. However, as we can see from Figure 7b, the average speed of vehicles did not affect the time delay for both compared algorithms.

On the other hand, Figure 7c illustrates the throughput comparison between the secure and insecure versions of the ITLCS for different numbers of vehicles. As we can see directly from the figure, the secure version required more throughput (i.e., 10%). More throughput was also consumed for more traveling vehicles for both algorithms. Figure 7d illustrates the throughput for both algorithms when the traffic speed changed while the number of vehicles stayed the same. As illustrated in the figure, the throughput did not change when changing the traffic speed.



(**a**) Processing time delay for different numberss of vehicles (**b**) Processing time delay time for different vehicle speeds

(**c**) Throughput for different numbers of vehicles (**d**) Throughput for different vehicle speeds

Figure 7. Efficiency of CITLCS.

7. Conclusions

The paper proposed a confidential intelligent traffic light control system to prevent unauthorized traceability. This system incorporated an attribute-based encryption mechanism to ensure privacy and security, which used a set of public attributes as the basis for fine-grained resource protection. The experimental results showed that the proposed system had a 100% success rate in preventing traceability attacks in different tested scenarios. However, it increased the processing time delay by 30% on average and the throughput by 10% compared to the insecure version of the system. The overhead caused by the proposed secure algorithm is manageable since the extra time delay is acceptable compared to the traffic speed, causing the vehicle to travel only a very short distance in the extra required milliseconds. Moreover, the extra required overhead in the throughput is negligible compared to the high available bandwidth of the VANET technology. This protocol encourages and motivates the traveling vehicle to participate in the data-gathering process without witnessing any traceability or linkability threats. In future studies, we aim to investigate how to extend the scalability of the proposed work, studying other attacks that can be eliminated by the proposed algorithm. We will also check how to modify the message size or change the selected encryption algorithms to enhance the performance and reduce the overhead.

Author Contributions: Conceptualization, M.B.Y. and S.G.; methodology, A.A., M.B.Y. and M.Y.; software, M.Y., A.A. and M.B.Y.; validation, M.B.Y., M.Y. and A.A.; formal analysis, S.G.; investigation, A.A. and M.B.Y.; resources, A.A. and M.B.Y.; data curation, M.Y. and A.A.; writing—original draft preparation, M.Y. and A.A.; writing—review and editing, M.B.Y.; visualization, M.Y., A.A. and M.B.Y.; supervision, M.B.Y. and S.G.; project administration, M.B.Y. and S.G.; funding acquisition, M.B.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used in this experimental study will be available on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Song, K.; Ni, T.; Song, L.; Xu, W. Emma: An accurate, efficient, and multi-modality strategy for autonomous vehicle angle prediction. *Intell. Converg. Netw.* **2023**, *4*, 41–49. [CrossRef]
2. Hu, S.; Tao, Y.; Xu, G.; Deng, Y.; Chen, X.; Fang, Y.; Kwong, S. Cp-guard: Malicious agent detection and defense in collaborative bird's eye view perception. In Proceedings of the AAAI Conference on Artificial Intelligence, Philadelphia, PA, USA, 25 February–4 March 2025; Volume 39, pp. 23203–23211.
3. Qiao, J.; Zhang, D.; de Jonge, D. Priority-based traffic management protocols for autonomous vehicles on road networks . In Proceedings of the AI 2021: Advances in Artificial Intelligence: 34th Australasian Joint Conference, Sydney, NSW, Australia, 2–4 February 2022; Springer International Publishing: Cham, Switzerland, 2022; pp. 240–253.
4. Gaouar, N.; Lehsaini, M.; Nebbou, T. CCITL: A cloud-based smart traffic management protocol using intelligent traffic light system in VANETs. *Concurr. Comput. Pract. Exp.* **2023**, *35*, e7686. [CrossRef]
5. Li, Z.; Yu, H.; Zhang, G.; Dong, S.; Xu, C.Z. Network-wide traffic signal control optimization using a multi-agent deep reinforcement learning. *Transp. Res. Part Emerg. Technol.* **2021**, *125*, 103059. [CrossRef]
6. Younes, M.B.; Boukerche, A. A performance evaluation of a context-aware path recommendation protocol for vehicular ad-hoc networks. In Proceedings of the 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA, 9–13 December 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 516–521.
7. Rapelli, M.; Casetti, C.; Sgarbi, M. A Distributed V2V-Based Virtual Traffic Light System. In Proceedings of the 2020 International Conference on COMmunication Systems and NETworkS (COMSNETS), Bangalore, India, 7–11 January 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 122–128.
8. Eom, M.; Kim, B.I. The traffic signal control problem for intersections: A review. *Eur. Transp. Res. Rev.* **2020**, *12*, 1–20. [CrossRef]
9. Cao, M.; Li, V.O.; Shuai, Q. Gain with no pain: Exploring intelligent traffic signal control for emergency vehicles. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 17899–17909. [CrossRef]
10. Pinto, A.C.; Mattioli, G.V. *Intelligent Traffic Lights Control System Using Fuzzy Logic (No. 2014-36-0359)*; SAE Technical Paper; SAE International: Warrendale, PA, USA, 2014.
11. Hossan, S.; Nower, N. Fog-based dynamic traffic light control system for improving public transport. *Public Transp.* **2020**, *12*, 431–454. [CrossRef]
12. Ximenes, D.S.; Simões, T.; Silva, A.C.d.; Martino, G.P.d.; Emiliano, W.M.; Menzori, M.; Meyer, Y.A.; Júnior, V.E.M. Vehicular Traffic Flow Detection and Monitoring for Implementation of Smart Traffic Light: A Case Study for Road Intersection in Limeira, Brazil. *Future Transp.* **2024**, *4*, 1388–1401. [CrossRef]
13. Younes, M.B.; Boukerche, A.; Mammeri, A. Context-aware traffic light self-scheduling algorithm for intelligent transportation systems. In Proceedings of the 2016 IEEE Wireless Communications and Networking Conference, Doha, Qatar, 3–6 April 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–6.
14. Sachan, A.; Kumar, N. Intelligent Traffic Control System for Emergency Vehicles. In *IoT and Analytics for Sensor Networks: Proceedings of ICWSNUCA 2021*; Springer: Singapore, 2022; pp. 151–160.
15. Younes, M.B.; Boukerche, A. Intelligent traffic light controlling algorithms using vehicular networks. *IEEE Trans. Veh. Technol.* **2015**, *65*, 5887–5899. [CrossRef]
16. Khalid, T.; Khan, A.N.; Ali, M.; Adeel, A.; ur Rehman Khan, A.; Shuja, J. A fog-based security framework for intelligent traffic light control system. *Multimed. Tools Appl.* **2019**, *78*, 24595–24615. [CrossRef]
17. Liu, J.; Li, J.; Zhang, L.; Dai, F.; Zhang, Y.; Meng, X.; Shen, J. Secure intelligent traffic light control using fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 817–824. [CrossRef]
18. Elsagheer Mohamed, S.A.; AlShalfan, K.A. Intelligent traffic management system based on the internet of vehicles (IoV). *J. Adv. Transp.* **2021**, *2021*, 1–23. [CrossRef]
19. Habib, M.A.; Ahmad, M.; Jabbar, S.; Khalid, S.; Chaudhry, J.; Saleem, K.; Khalil, M.S. Security and privacy based access control model for internet of connected vehicles. *Future Gener. Comput. Syst.* **2019**, *97*, 687–696. [CrossRef]
20. Younes, M.B.; Boukerche, A. SCOOL: A secure traffic congestion control protocol for VANETs. In Proceedings of the 2015 IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, USA, 9–12 March 2015; pp. 1960–1965.

21. Younes, M.B.; Alonso, G.R.; Boukerche, A. A distributed infrastructure-based congestion avoidance protocol for vehicular ad hoc networks. In Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 73–78.
22. Alharbi, A.; Halikias, G.; Sen, A.A.A.; Yamin, M. A framework for dynamic smart traffic light management system. *Int. J. Inf. Technol.* **2021**, *13*, 1769–1776. [CrossRef]
23. Gupta, S.; Zhang, Y.; Su, R. Urban traffic light scheduling for pedestrian–vehicle mixed-flow networks using discrete sine–cosine algorithm and its variants. *Appl. Soft Comput.* **2022**, *120*, 108656. [CrossRef]
24. Sun, G.; Qi, R.; Liu, Y.; Xu, F. A dynamic traffic signal scheduling system based on improved greedy algorithm. *PLoS ONE* **2024**, *19*, E0298417. [CrossRef]
25. Aleko, D.R.; Djahel, S. An efficient adaptive traffic light control system for urban road traffic congestion reduction in smart cities. *Information* **2020**, *11*, 119. [CrossRef]
26. Jin, Q. Automatic Control of Traffic Lights at Multiple Intersections Based on Artificial Intelligence and ABST Light. *IEEE Access* **2024**, *12*, 103004–103017. [CrossRef]
27. Wided, A.; Assia, B.; Fatima, B. Traffic Management system and Traffic Light Control in Smart City to Reduce Traffic Congestion. *Int. J. Autom. Amart Technol.* **2023**, *13*, 2464. [CrossRef]
28. Sihwail, R.; Ibrahim, D. A New Image Encryption Method Using an Optimized Smart Codebook. *Hum. Behav. Emerg. Technol.* **2025**, *2025*, 7807003. [CrossRef]
29. Ibrahim, D.; Sihwail, R.; Arrifin, K.A.Z.; Abuthawabeh, A.; Mizher, M. A novel color visual cryptography approach based on Harris Hawks Optimization Algorithm. *Symmetry* **2023**, *15*, 1305. [CrossRef]
30. Mizher, M.A.A.J.A.; Sulaiman, R.; Abdalla, A.M.A.; Mizher, M.A.A. A simple flexible cryptosystem for meshed 3D objects and images. *J. King Saud-Univ.-Comput. Inf. Sci.* **2021**, *33*, 629–646. [CrossRef]
31. Mizher, M.A.; Sihwail, R.; Baker, M.B.; Mazhar, A.A.; Mizher, M.A.; Ibrahim, D. A review of cybersecurity for internet-of-things based on next generation healthcare networks. *AIP Conf. Proc.* **2023**, *2979*, 070004.
32. Said, S.O.; Sihwail, R.; Shehadeh, H.; Hashim, I.; Alieyan, K. Hybrid Newton–sperm swarm optimization algorithm for nonlinear systems. *Mathematics* **2023**, *11*, 1473. [CrossRef]
33. Feng, Y.; Huang, S.; Chen, Q.A.; Liu, H.X.; Mao, Z.M. Vulnerability of traffic control system under cyberattacks with falsified data. *Transp. Res. Rec.* **2018**, *2672*, 1–11. [CrossRef]
34. Chen, C.; Wei, H.; Xu, N.; Zheng, G.; Yang, M.; Xiong, Y.; Xu, K.; Li, Z. Toward a thousand lights: Decentralized deep reinforcement learning for large-scale traffic signal control. In Proceedings of the AAAI Conference on Artificial Intelligence, New York, NY, USA, 7–12 February 2020; Volume 34, pp. 3414–3421.
35. Kumar, N.; Rahman, S.S.; Dhakad, N. Fuzzy inference enabled deep reinforcement learning-based traffic light control for intelligent transportation system. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 4919–4928. [CrossRef]
36. Zheng, G.; Xiong, Y.; Zang, X.; Feng, J.; Wei, H.; Zhang, H.; Li, Z. Learning phase competition for traffic signal control. In Proceedings of the 28th ACM International Conference on Information and Knowledge Management, Beijing, China, 3–7 November 2019; pp. 1963–1972.
37. Liang, X.; Du, X.; Wang, G.; Han, Z. A deep reinforcement learning network for traffic light cycle control. *IEEE Trans. Veh. Technol.* **2019**, *68*, 1243–1253. [CrossRef]
38. Shinde, S.M. Adaptive traffic light control system. In Proceedings of the 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM), Aurangabad, India, 5–6 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 300–306.
39. Wang, Y.; Yang, X.; Liang, H.; Liu, Y. A review of the self-adaptive traffic signal control system based on future traffic environment. *J. Adv. Transp.* **2018**, *2018* . [CrossRef]
40. Yousef, K.M.; Al-Karaki, M.N.; Shatnawi, A.M. Intelligent traffic light flow control system using wireless sensors networks. *J. Inf. Sci. Eng.* **2010**, *26*, 753–768.
41. Rezgui, J.; Barri, M.; Gayta, R. Smart traffic light scheduling algorithms. In Proceedings of the 2019 International Conference on Smart Applications, Communications and Networking (SmartNets), Sharm El Sheik, Egypt, 17–19 December 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–7.
42. Liu, C.; Ke, L. Cloud assisted Internet of things intelligent transportation system and the traffic control system in the smart city. *J. Control Decis.* **2023**, *10*, 174–187. [CrossRef]
43. Yuan, S.; Li, H.; Han, X.; Xu, G.; Jiang, W.; Ni, T.; Zhao, Q.; Fang, Y. ITPatch: An Invisible and Triggered Physical Adversarial Patch against Traffic Sign Recognition. *arXiv* **2024**, arXiv:2409.12394.
44. Yuan, S.; Xu, G.; Li, H.; Zhang, R.; Qian, X.; Jiang, W.; Cao, H.; Zhao, Q. FIGhost: Fluorescent Ink-based Stealthy and Flexible Backdoor Attacks on Physical Traffic Sign Recognition. *arXiv* **2025**, arXiv:2505.12045.
45. Alqarqaz, M.; Younes, M.B.; Qaddoura, R. An object classification approach for autonomous vehicles using machine learning techniques. *World Electr. Veh. J.* **2023**, *14*, 41. [CrossRef]

46. Arshad, H.; Johansen, C.; Owe, O.; Picazo-Sanchez, P.; Schneider, G. Semantic Attribute-Based Encryption: A framework for combining ABE schemes with semantic technologies. *Inf. Sci.* **2022**, *616*, 558–576. [CrossRef]
47. Aldolimi, W.S.; Hnaif, A.A.; Alia, M.A. Light fidelity to transfer secure data using advanced encryption standard algorithm. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 963–967.
48. Rehmani, M.H.; Saleem, Y. Network simulator NS-2. In *Encyclopedia of Information Science and Technology*, 3rd ed.; IGI Global: Hershey, PA, USA, 2015; pp. 6249–6258.
49. Nawej, C.; Owolawi, P.; Walingo, T. Design and simulation of vanets testbed using openstreetmap, sumo, and ns-2. In Proceedings of the 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS), Chengdu, China, 23–26 April 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 582–587.
50. Kusari, A.; Li, P.; Yang, H.; Punshi, N.; Rasulis, M.; Bogard, S.; LeBlanc, D.J. Enhancing SUMO simulator for simulation based testing and validation of autonomous vehicles. In Proceedings of the 2022 IEEE Intelligent Vehicles Symposium (IV), Aachen, Germany, 4–9 June 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 829–835.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.