sensors

MDPI

Article

Secure and Efficient High Throughput Medium Access Control for Vehicular Ad-Hoc Network

Mohammed Abdulhakim Al-Absi [1], Ahmed Abdulhakim Al-Absi [2,*], Rui Fu [3], Ki-Hwan Kim [4], Young-Sil Lee [4], Byung-Gook Lee [5], Sang-Gon Lee [5] and Hoon-Jae Lee [5,*]

1 Department of Computer Engineering, Graduate School, Dongseo University, Busan 47011, Korea; d0185123@kowon.dongseo.ac.kr
2 Department of Smart Computing, Kyungdong University, Gosung 24764, Korea
3 Blockchain Laboratory of Agricultural Vegetables, Weifang University of Science and Technology, Weifang 262700, China; furui19891209@wfust.edu.cn
4 International College, Dongseo University, Busan 47011, Korea; ghksdl90@naver.com (K.-H.K.); youngsil.lee0113@gmail.com (Y.-S.L.)
5 Division of Information and Communication Engineering, Dongseo University, Busan 47011, Korea; lbg@dongseo.ac.kr (B.-G.L.); nok60@gdsu.dongseo.ac.kr (S.-G.L.)
* Correspondence: absiahmed@kduniv.ac.kr (A.A.A.-A.); hjlee@dongseo.ac.kr (H.J.L.)

Abstract: The evolution of the internet has led to the growth of smart application requirements on the go in the vehicular ad hoc network (VANET). VANET enables vehicles to communicate smartly among themselves wirelessly. Increasing usage of wireless technology induces many security vulnerabilities. Therefore, effective security and authentication mechanism is needed to prevent an intruder. However, authentication may breach user privacy such as location or identity. Cryptography-based approach aids in preserving the privacy of the user. However, the existing security models incur communication and key management overhead since they are designed considering a third-party server. To overcome the research issue, this work presents an efficient security model namely secure performance enriched channel allocation (S − PECA) by using commutative RSA. This work further presents the commutative property of the proposed security scheme. Experiments conducted to evaluate the performance of the proposed S − PECA over state-of-the-art models show significant improvement. The outcome shows that S − PECA minimizes collision and maximizes system throughput considering different radio propagation environments.

Keywords: V2V; authentication; security; DSRC; privacy; MAC

Citation: Al-Absi, M.A.; Al-Absi, A.A.; Fu, R.; Kim, K.-H.; Lee, Y.-S.; Lee, B.-G.; Lee, S.-G.; Lee, H.-J. Secure and Efficient High Throughput Medium Access Control for Vehicular Ad-Hoc Network. *Sensors* **2021**, *21*, 4935. https://doi.org/10.3390/s21144935

Academic Editors: Lei Zhang, Weizhi Meng and Kaitai Liang

Received: 1 June 2021
Accepted: 9 July 2021
Published: 20 July 2021

1. Introduction

VANET is a special type of Mobile ad hoc Network (MANET) where vehicles/devices act mobile devices, and their mobility is defined by network road topologies [1]. The goal of VANET is to assist drivers and subscribers with a reliable and safe atmosphere. The communication in VANET takes place from Vehicle to Infrastructure (V2I), Vehicle to Vehicle (V2V), and Vehicle to Everything (V2X) which is a combination of both. Each vehicle is equipped with sensors such as onboard unit (OBU), Bluetooth, 3G/4G/5G, and Wi-Fi that has communication and computational capabilities [2] (Table 1). Roadside unit (RSU) with dedicated short-range communication (DSRC) [3,4] is the public infrastructure that is fixed on the roadside to provide internet to the vehicle [5,6]. A typical VANET communication is shown in Figure 1. DSRC is a dedicated short-range communication, which is a one-way or two-way short-range to medium-range wireless communication technology based on the IEEE802.11p protocol [7,8]. In October 1999, the United States Federal Communications Commission (FCC) allocated 75 MHz of spectrum in the 5.9 GHz frequency band for use by Intelligent Transportation Systems (ITS) [9], which is now one of the two technologies that implement V2X [10].

Table 1. Communication technologies in VANET [2].

Technology	Type	Distance
2G/3G/4G/5G	Duplex	Global
Bluetooth	Simplex	≈10 m
WiMAX	Duplex	≈1 km
GPS	Simplex	global
ZigBee	Duplex	≈20 m
DSRC 802.11p/WAVE	Duplex	≈1 km
Wi-Fi	Duplex	≈50 m
RFID	Simplex	10 m

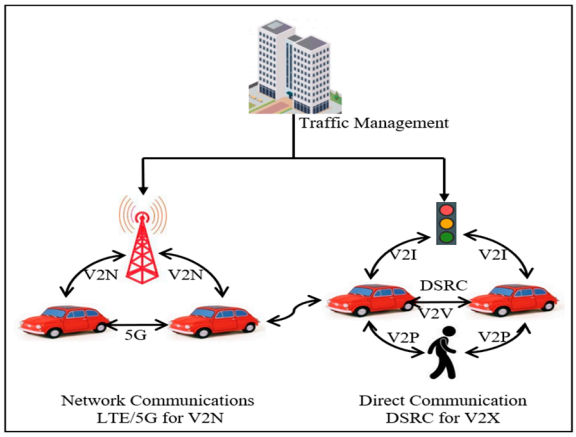

Figure 1. The architecture of vehicular ad hoc communication.

DSRC adopts the IEEE 802.11p standard specification for wireless communication [11], where each device broadcast a safety-related message every 100–300 milliseconds, which possess vehicle driving-related data, such as speed, location, and driving status (e.g., waiting for the signal, regular driving, traffic jam, etc.), to neighboring devices. With the acquired information, other vehicles can make a timely decision in cases such as traffic jams, emergent braking, and accidents. As mentioned in Figure 2, works at the media access control and physical layers act strictly, and it is worth noting that IEEE 802.11p is limited by the scope of IEEE 802.11. The operational functions and complexity of DSRC are taken care of by upper layers of IEEE 1609 standards. Based upon management activities defined in IEEE P1609.1, the security protocols defined in IEEE P1609.2 and the network-layer protocol defined in IEEE P1609.3, the applications utilized in the WAVE environment are depicted by these standards. Compared to 802.11p, IEEE 1609.4 is higher in level, and the operation of higher layers without the necessity the physical channel access parameters is supported [12].

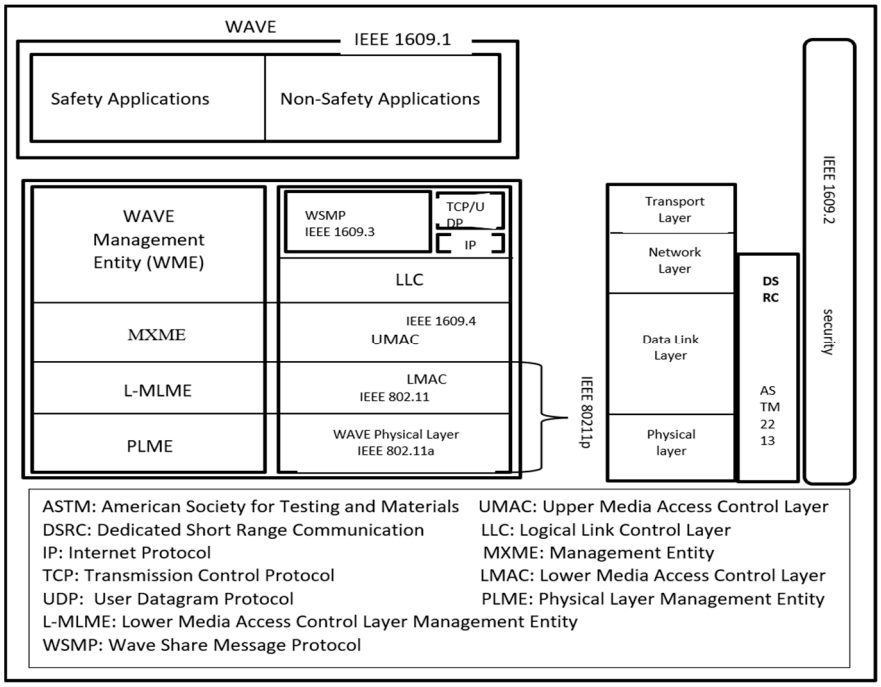

Figure 2. WAVE model.

The DSRC ecosystem has implemented various functions and fully tested V2X applications for more than ten years [13]. However, DSRC provides a complete set of interoperable solutions [14,15]. The key advantage of DSRC is that it can "see the surrounding corners" without other sensors. DSRC technology with high mobility can handle rapidly changing environments at a speed of up to 500 km/h even if an obstacle is suddenly detected, and its range exceeds 1 km [16,17]. DSRC makes it possible for users of the road to be connected, which guarantees the reliability of V2V and V2I. The European Commission believes that the use of this technology is expected to reduce the probability of local motor vehicle accidents to zero in 2050 [18].

C − V2X is a wireless communication technology for cellular vehicles. At present, the market is upgrading to 4GC − V2X, and 5GC − V2X is in the process of standardization [19]. In the future, it will arrive at the same time as the implementation of intelligent vehicle interconnection. C − V2X is supported by many mobile operators, major mobile device manufacturers, and automakers, including Audi, BMW, Daimler, Ford, Tesla, and Toyota. Mobile operators, equipment suppliers, and vehicle manufacturers are joining forces to test C − V2X [20,21].

Though VANET offers tremendous benefits, at the same time, Internet of Vehicles (IoVs) are prone to security attacks. As a result, the security issues must be addressed before practical usage [22]. Therefore, recently, extensive research on network security protocols has been carried considering characteristics such as highly dynamic and self-organizing network topology which is applied to IoV. Among them, identity authentication methodology is an effective way to provide data security [23]. Similarly, authentication and key management techniques have been widely studied and applied extensively in other fields such as the Internet of things (IoT), smart grids, mobile cloud computing, etc. [24–26]. The desired security on such a platform must first guarantee message integrity. Secondly, to prevent impersonation attacks, the data sender must be authenticated. In addition, user privacy [7,27] concerns must be taken care of, where the position, identity, and movement of a particular user must not be accessible to any third party. However, in VANET, it is not desired to have such an unconditional privacy-preserving scheme. Since the malicious/intruder vehicles must be tracked and punished in case of any malicious activity carried out.

The authentication scheme can be broadly classified into the following three categories: cryptography-based [28,29], trust-based [30,31], and hardware-based [32,33]. In the V2V semi-trust model, organizations involved in protecting privacy are not well suited to deliver high-throughput security applications and smart entertainment applications. To protect the confidentiality of user information, many studies on the state of the art mainly use encryption technology. The encryption technology is mainly based on symmetric or asymmetric encryption keys and decryption. We review the use of secure servers or third-party servers as traditional methods of computing and distributing the key to an authorized organization [34].

The authorities involved in preserving privacy in V2V semi-honest trust model are not suitable for provisioning high throughput safety and smart infotainment application. To preserve the privacy of user data, in literature, many researchers have predominantly adopted cryptography techniques. The cryptography technique relies on the keys for encryption and decryptions, where keys are symmetric or asymmetric. To compute keys and distribute among authorities, a secure or third-party server is considered [35,36]. The usage of third-party servers incurs the overhead of key computation, storage, and distribution, also known as the initialization phase. Post completion of the initialization phase, the message is secured using cryptography and is shared among vehicles. The design of the proposed Secure Performance Enriched Channel Allocation ($S-PECA$) model aims to eliminate the need for the local message available with the authorities to be released for provisioning high throughput safety and infotainment application. Firstly, we develop an efficient MAC namely PECA [37] that overcomes the $NP-$hard problem [38] of channel sharing in ENCCMA [39] MAC design. Secondly, a security model is designed using commutative RSA, namely, $S-PECA$.

The contributions of this research paper are:

- RSA cryptography technique with commutative key helps maintain message integrity and privacy.
- Our proposed scheme minimizes the computational overheads associated with preserving the privacy of the $S-PECA$ model (namely key computation, exchange, and distribution using external entities).
- The $S-PECA$ model preserves or protects the privacy information in the presence of untrusted or dishonest authorities.
- Compared with the existing design, the provision of our design has a much lower security overhead.
- The result obtained shows that the suggested design minimizes collision and maximizes system throughput.

The remainder of the work is as follows. In Section 2, the literature review is carried out. The proposed channel allocation model is discussed in Section 3. In the penultimate section, experiments and simulations are presented. The last section provided and discussed the conclusion with future work.

2. Literature Review

A comprehensive survey of the existing security design is carried out for provisioning security to VANET in this section. In [35] presented an efficient pseudonymous authentication design to protect user personal information. They presented multiple hierarchies of pseudonyms based on user sessions. A session with smaller timestamp pseudonyms is used for communication among semi-trusted authorities and longer session timestamp pseudonyms are used for communication among vehicles. Their model overcomes the storage and computation overhead of certificate revocation lists and group-based approaches. Experimental outcomes show it minimizes end-to-end package delay and delivery ratio. However, they consider only honest but curious server and suffer from trust-related issues concerning certificate authority. The study in [40] proposes a geo-routing protocol for the introduction of the Location Errors Record (LER-GR), evaluating the position error of neighboring vehicle compounds using the error calculation method according to the Rayleigh

distribution and development of position prediction and correction technology based on Kalman filter and prediction of the position of neighboring vehicles. The authors in [41] use the reconfigurable intelligent surface (RIS) to enhance the Physical Layer Security (PLS) in VANET. However, they have presented two network system models: the first is vehicle-to-vehicle communication through RIS and source-based access points, and the second is information of VANET with RIS based relay deployed in the building as mentioned in [42]; the signature verification takes around 20 ms by the onboard unit at a 400 MHz processor. This might not be a problem in sparse areas, but in dense areas, it could cause significant delays in the message verification process. The Certificate Revocation List (CRL) is another limitation of the pseudonym methods, i.e., certification authority creates a set of public vehicle key certificates. Then, the vehicle uses the private key to sign the beacon and broadcasts the signal using the corresponding public key certificate. However, in the case of revocation, you need to add all certificates of revoked users to the CRL. Hybrid Intrusion Detection System (D2H-IDS) is used to separate trusted service requests from invalid requests that were created during malicious attacks used to prevent security attacks [43]. Reference [44] designed an approach to optimize scheduling, routing, and access control while reducing network congestion, securing a slot allocation for reserved traffic, securing network reliability, and maximizing approval of network flows. Reference [45] presented a reliable and secure connection to reduce unnecessary communication between edges by relying on the transport protocol between nodes in smart cities. Reference [46] proposed HIBS-K Sharing, given different types of communication devices, which is suggested to share a hierarchical identifier-based signature key for Automotive vehicles. Similarly, the authors in [47] presented a hardware-based security design to provide security to address the trust-related issue of [35]. They considered a hybrid security model and presented a design to preserve the privacy of vehicular communication. Their model considers dual authentication based on different IoV scenarios. Firstly, the onboard unit computes a temporary encryption key and anonymous identity to initialize the authentication session. Then, the trusted authority can evaluate the authorized vehicles' anonymous and real identities. The vehicle reputation is evaluated based on past transmission based on which a session key can be established. Their model preserves privacy and minimizes key exchange overhead. Nonetheless, the tamper-proof device may not guarantee all the VANET security requirements [36] and incurs communication overhead. To address this, ref. [36] presented a secure privacy-preserving authentication scheme. Their model does not rely on any hardware and attained a much higher data rate than the batch verification scheme by using the binary search method and cuckoo filter. They have achieved a great improvement in performance over the state-of-the-art technique. Since it is paired for free, the mapping point segmentation function is not used. An extensive survey carried shows the cryptography approach plays a significant in preserving the user and adopting third-party servers and public-key cryptography incurs communication and key management overheads. To address research challenges, in the next section, we present a secure MAC design using commutative RSA.

3. Secure VANET Communication (SVC) Using Commutative RSA Technique

This work presents a secure MAC protocol design for VANET. Firstly, we present a Perform Enriched Channel Algorithm (PECA) for the shared channel and the non-shared channel in VANET. First, we choose the best channel available to the user according to the throughput gain requirements. The users do not share channels here; the user enters the channel during a specified period and leaves the channel so that other users can access it. However, this algorithm cannot use the bandwidth effectively. This is because the channels are not shared. To solve this problem, the second algorithm proposes a shared channel allocation algorithm. Here, a group of users shares channels between neighboring users. This algorithm utilizes bandwidth efficiently, which aids in minimizing collision and maximize system throughput Then we present a CRSA based security design $S-PECA$

for secure communication among vehicles. The list of notations and symbols used in this paper is given in Table 2.

Table 2. Variable notation.

Notations	Abbreviation
x	Vehicle
C_x	Throughput Achieved
e_{xy}	Channel allocation decision
y	Channel
V_x	Channel set allocated to vehicle x
l_{xy}	The likelihood for channel y accessibility
$1 - \prod_{y \in V_x} l'_{xy}$	The likelihood for channel y accessibility for at most one channelpt
l'_{xy}	The likelihood that channel y is not accessible
δC_x	Throughput increment
V_z	The input set of accessible channels
C_x^z	Throughput before channel allocation y'_x.
C_x^q	Throughput after channel allocation y'_x.
T	Is the total number of channels in the network
$l'_{xy} = 1 - l_{xy}$	Is the probability of vehicle x not accessing the channel y
y'_x	channel allocation
$1 - \prod_{y \in T_x} l'_{xy}$	Is the probability of x vehicle accessing the channel
$\mathcal{D}$	MAC Overhead
$\mathbb{V}$	Number of vehicles
$\mathbb{T}$	The sharing vehicles of channel y
s	Is the common shared channel
n	The shared channel user number
m	Is the user's number using the shared channel
$\prod_{m=1, m \neq n}^{\mathbb{T}} l_{x_m y}$	Is the likelihood computation of throughput gain on a shared user channel
$\mathcal{R}_X$and $\mathcal{R}_Y$	The region member required to securely communicate over the secure channel
j	Vehicle
P_j	A set of channels shared by j
F_y	Group of vehicles who share channel y
P_o	A set of channels shared by o vehicle
$\mathcal{A}$	contention window
$\mathcal{L}_u$	Likelihood of the first collision
ϵL	likelihood tradeoff
r	No. of vehicles
g	Arbitrary back-off time
$\mathcal{L}_u^{(r)}$	Condition likelihood of the first collision
$\mathbb{L}\{r \ vehicle \ contend\}$	The likelihood that r vehicles participate in the contention phase

Table 2. *Cont.*

Notations	Abbreviation
$\wedge_R$	Set of all R vehicles $(\{1,2,3,\ldots,R\})$
$\wedge_t$	A specific set of r user
h	Mean value of the back-off parameter
$\mathcal{D}(\mathcal{A})$	Mean Overhead
s_{CTS}	Corresponding time of CTS
s_{RTS}	Corresponding time of RTS
s_{SIFS}	Corresponding time of SIFS
s_{SYNC}	Size of synchronization packets
s_{SEN}	Time of sensing
φ	A time that corresponds to one back off param
$S_{\mathcal{I}}$	Cycle Time
A_a^c	Prime Number
B_b^c	Prime Number
$\mathcal{E}^c$	Public Key
$\mathcal{D}^c$	Secret Key
U	Data
$\mathcal{Y}$	EncData
$\mathbb{D}_V$	Decryption EncData

(a) Non-shared channel allocation (NSCA):

Where T_x defines the channels assigned to vehicle/node x ($T_x \cap T_y = \varnothing, x \neq y$); $l_{x,y}$ is the likelihood that channel y is accessible at vehicle x. The mechanism of the non-channel shared allocation algorithm (if each participant is given a channel to transmit in a specified time, it is called Non- Shared Channel Algorithm) allows the vehicle to be allocated channels repeatedly to maximize throughput. However, in each channel frequency, each x vehicle will calculate the throughput gain when assigning the best channel under the following condition

$$y'_x = \underset{y \in T_z}{argmax} l_{x,y}, \tag{1}$$

This throughput Gain is calculated as

$$\delta C_x = C_x^z - C_x^q = \left[1 - \left(1 - l_{xy'_x}\right) \prod_{y \in T_x} \left(1 - l_{xy}\right)\right] - \left[1 - \prod_{y \in T_x} \left(1 - l_{xy}\right)\right] = l_{xy'_x} \prod_{y \in T_x} \left(1 - l_{xy}\right) \tag{2}$$

It can be noticed from Equation (2), δC_x is reduced with each repetition of the assignment, where C_x^z and C_x^q are the throughputs before and after channel, T is the total number of channels in the network, and if T_x increases, then $\prod_{y \in T_x} \left(1 - l_{xy}\right)$ tends to zero. However, given this situation, the recommended NSCA is defined in flow diagram 1 as shown in Figure 3. First, we initialize the set available channel for all vehicles, then for all vehicles do allocate the best available channel to the vehicle (a channel with maximum likelihood). Then, check if the set of channels assigned to the vehicle is not equal to zero. If it is not equal to zero, then, obtain throughput gain before and after channel allocation. If it is equal to zero, then, the likelihood of throughput gain is assigned. Assign each vehicle maximum throughput, and then, allocate channel with maximum throughput to vehicles. Update the allocated channel information with maximum throughout to each vehicle. If the allocated channel is empty, then, terminate, or else go to step 2.

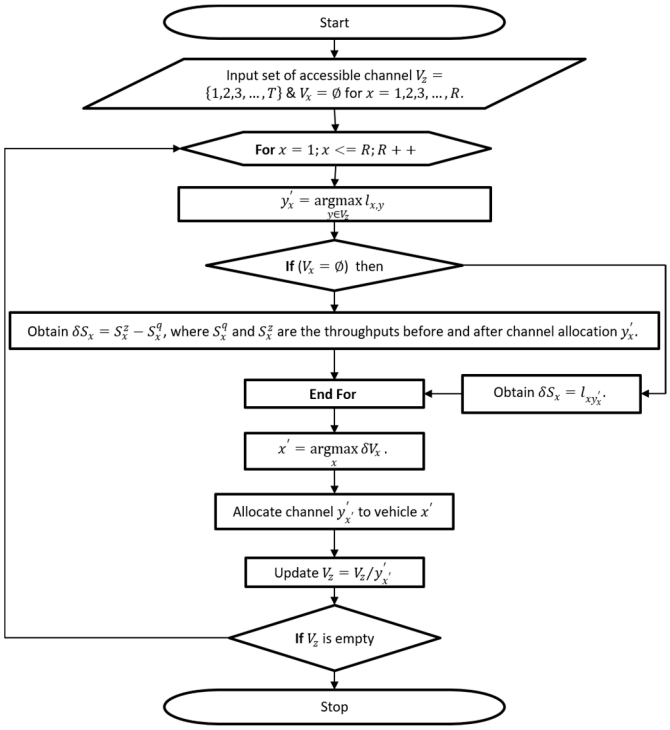

Figure 3. Flow diagram of proposed non-shared channel allocation.

Note: we run flow diagram 1, to get channels set assigned to each device/vehicle, and according to these channels, Equation (5) can be utilized to calculate the throughput. Therefore, this work's goal is to achieve maximum throughput in the network to obtain channel allocation performance. However, we consider the throughput gained by x vehicle/device where C_x and e_{xy} represent the channel allocation decision. However, if the y channel is set for x vehicle, e_{xy} is set 1, else e_{xy} is set to 0. However, the gain throughput issue is shown as follows:

$$\max_{E} \sum_{x}^{R} C_x. \tag{3}$$

We have the following commitment to allocate the non-shared channel as

$$\sum_{x}^{R} e_{xy} = 1 \ \forall y \tag{4}$$

Now, we can calculate the throughput gained by x vehicle on non-shared channel assignment according to the following formula: T_x is the x vehicle/device assigned channel group, and l_{xy} is x vehicle channel y accessibility. However, C_x is calculated as follows:

$$C_x = 1 - \prod_{y \in T_x} l'_{xy} = 1 - \prod_{y=1}^{K} \left(l'_{xy} \right)^{e_{xy}} \tag{5}$$

where $l'_{xy} = 1 - l_{xy}$ is the probability of x vehicle/device not accessing the y channel, and $1 - \prod_{y \in T_x} l'_{xy}$ is the probability of x vehicle accessing the channel. However, each vehicle can use one channel utmost, so the highest throughput is 1. The bound in Equation (4) is not required in the channel assignment technique. Moreover, solving Equations (3) and (4) are NP − hard problems because this is a nonlinear integer program.

(b) Shared channel allocation (SCA):

A shared channel (If the channel is shared between neighboring vehicles, then each vehicle has a specific time to do the transmission. However, the time required to reach

the channel is determined by two factors, maximum throughput, and reduced collision for multi-user vehicle grid in the duct help improve throughput performance. However, they create MAC overhead due to multi-user allocation access channel conflict. Therefore, an optimized channel allocation method is needed to overhead for redundant design and balance throughput.

The channel allocation model includes two steps. In the first as shown in Figure 2, single-vehicle channel assignment information is computed using flowchart 1. The following deals with multi-user channel allocation by assigning channels assigned to specific vehicles to other vehicles. Here, we model the SCA algorithm as shown in flow chart 2 in Figure 4.

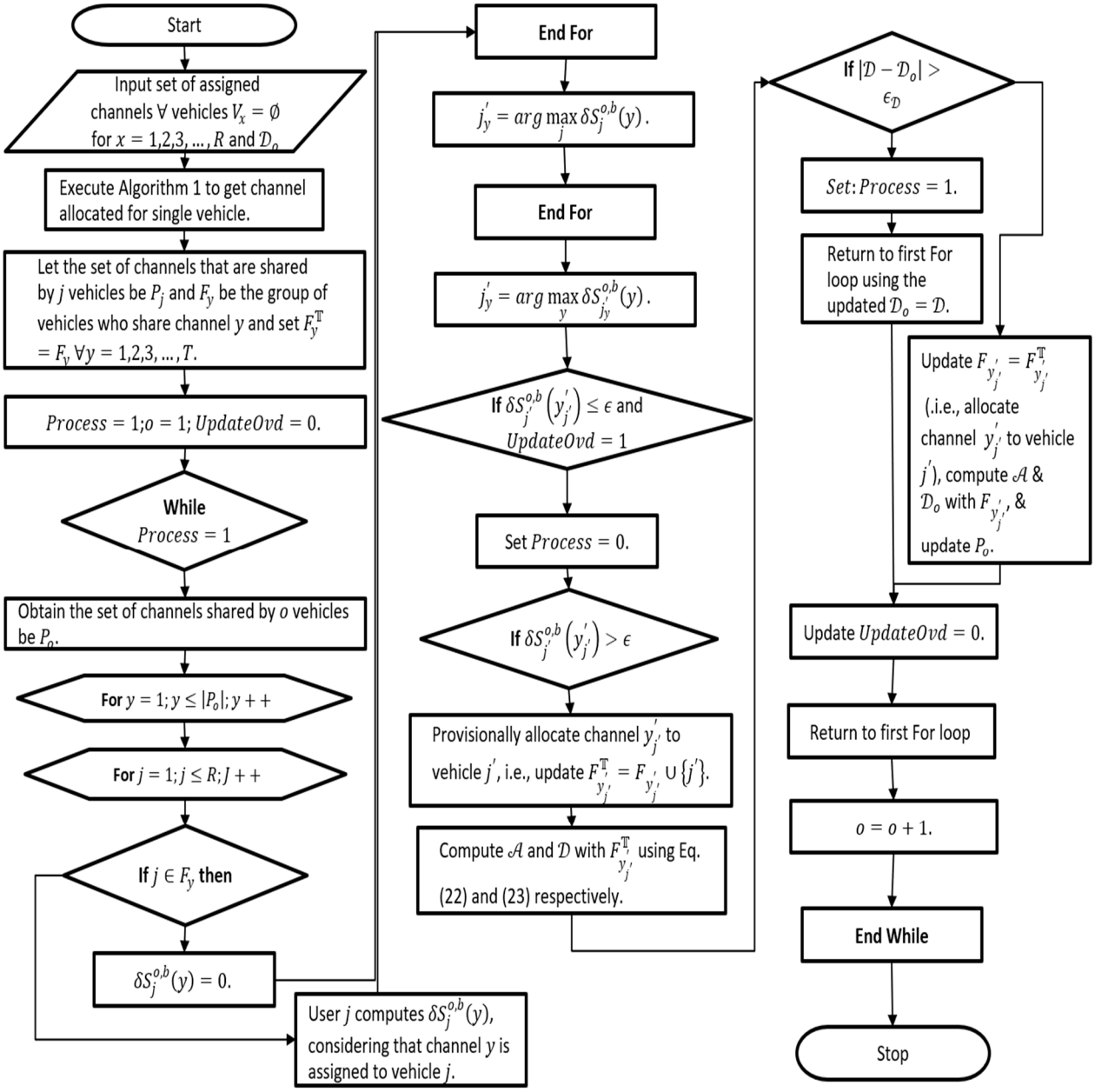

Figure 4. Flow diagram of proposed channel shared allocation.

First, assigned accessible channels for all vehicles. Execute algorithm to obtain channel assigned to single vehicle then consider a group of channels which are shared by set vehicles/device and set of vehicles that shares channel among vehicles in the network.

Update overhead to zero and set process to 1. Initialize the while loop and the options set of channels shared by vehicles. Initialize for loop for all shared vehicles in the network, and then, find if a vehicle belongs to the vehicle that shares their channel. If the channel is shared, then the assigned estimated throughput gain of the channel is zero; else, the vehicle computes throughout the gain considering the channel is allocated to vehicles. Assign estimated throughput gain for channel to the vehicle, and again, estimate throughput gain for the channel to the vehicle that shared the channel. If the estimated throughput gain is less than or equal to collision likelihood and overhead tradeoff, update overhead to 1 and set process to zero, and then, end the while. However, if the estimated throughput gain is greater than the collision likelihood, then provisionally allocates a channel to a vehicle that shares the available channel. Compute contention window and MAC overhead for the vehicle that shares the available channel. If the current MAC overhead is (minus initialized MAC overhead) greater than collision likelihood then, process overhead is set to 1. (Means it incurs MAC overhead as a result new channel need to be identified). Initialize the loop for all shared vehicles using updated MAC overhead. If the current MAC overhead is not greater than collision, then assign a channel to the shared vehicle. Compute MAC overhead and contention window and update group of channels shared by a set of vehicles. Update overhead to zero (no overhead is incurred in channel allocation of the shared channel) and increment the number of vehicles using the shared channel.

However, the calculation of indicators is a very difficult task. Therefore, by taking MAC overhead $\mathcal{D} < 1$, we calculate the channel allocation throughput gain. ($\mathcal{D}$ represents MAC overhead incurred in allocating a set of channels to the vehicle. The likelihood of collision due to the overhead incurred in the MAC layer due to channel allocation will be a range of 0 to 1.) Note: $\mathcal{D}$ overhead is based on the output of the channel assignment. The calculation of $\mathcal{D}$ is later described in the subsection of this paper.

Consider y channel is the channel shared in $x_1, x_2, \ldots, x_{\mathbb{T}}$ the vehicle, and $\mathbb{T}$ are the sharing vehicles of y channel. Here, if the y channel is assigned to a particular x vehicle, then we compute the gain throughput of that vehicle. If other vehicles $x_1,\ x_2, \ldots, x_{\mathbb{T}}$ do not use this y channel or are unreachable to the y channel, x vehicle can use the y channel which can increase throughput gain transmission when taken into consideration. The throughput gains of x vehicle and y channel are calculated as follows:

$$\delta C_x^{\mathbb{T},b}(y) = \left(1 - \frac{1}{\mathbb{T}}\right)(1-\mathcal{D}) l_{xy} \left(\prod_{o \in T_x} \bar{l}_{xo}\right) * \left(1 - \prod_{o \in T_*^s} \bar{l}_{xo}\right) \sum_{n=1}^{\mathbb{T}} \left[\bar{l}_{x_n y} \left(\prod_{m=1, m \neq n}^{\mathbb{T}} l_{x_m y}\right)\right] \tag{6}$$

where b is the estimated throughput gain of user and channel; $\bar{l}_{xo}$ is the number of users sharing the channel; $1 - \prod_{o \in T_*^s} \bar{l}_{xo}$ is the likelihood of the commonly shared channel users. s is the common shared channel; n is the shared channel user number; m is the user's number uses the shared channel; $\prod_{m=1, m \neq n}^{\mathbb{T}} l_{x_m y}$ is the likelihood computation of throughput gain on a shared user channel.

The S − ENCCMA model is implemented using the RSA with the commutative key mechanism. S − ENCCMA uses the ENCCMA real-time communication MAC protocol [37]. However, to provide access to real-time, ENCCMA combines Cognitive Radio, TDMA, and FDMA techniques. The ENCCMA MAC protocol can block signal transmission, and this aids to improve system efficiency. Therefore, ENCCMA does not consider user privacy, nor does it provide message authentication security. The proposed security model is presented in the next subsection.

(c) RSA with commutative key:

Generally, with encrypting, we first encrypt with Bob's key, then encrypt with Alice's key, and then decrypt with Alice's key and Bob's key. The exchange cipher allows decoding in any order. An important factor is that Bob and Alice need to share the values of p and q. For example, Figure 5 shows the encryption in the correct order and then in the incorrect order with the use of Prime size 128 (bits).

Figure 5. Encryption in the correct order and then in the incorrect order.

However, we propose a safe and effective CRSA algorithm for data authentication between participant's vehicles/devices in a V2V environment. To enable safe data communication among the corresponding vehicle in the V2V environment, it is a noble commutative RSA method which indicates that in order encryption can be performed in the same manner without affecting the results of encryption and decryption technique.

A secure communication model can be realized only when message transmitted over the communication channel is protected and cannot be collided. To achieve this, cryptography mechanisms are generally considered. Therefore, the S − PECA proposed here adopts CRSA algorithm. The S − PECA considers two prime param $A_a^{\mathcal{C}}$ and $B_b^{\mathcal{C}}$ initialized amongst all the vehicles of the region. Let $\mathcal{R}_X$ and $\mathcal{R}_Y$ represent the region member required to securely communicate over the secure channel. To compute the encryption keys and decryptions key pairs of the CRSA algorithm, the property $L^{\mathcal{C}}$ and $M^{\mathcal{C}}$ are evaluated using the following:

$$L^{\mathcal{C}} = \left[\left(A_a^{\mathcal{C}}\right) \times \left(B_b^{\mathcal{C}}\right)\right] \tag{7}$$

$$M^{\mathcal{C}} = \left[\left(A_a^{\mathcal{C}} - 1\right) \times \left(B_b^{\mathcal{C}} - 1\right)\right] \tag{8}$$

From the above expression, it can be seen that $L_X^{\mathcal{C}} = L_Y^{\mathcal{C}}$ and $M_X^{\mathcal{C}} = M_Y^{\mathcal{C}}$ for X and Y. The key pair for encryption of X and Y are signified as follows:

$$\left(L_X^{\mathcal{C}}, \mathcal{E}_X^{\mathcal{C}}\right) \text{ and } \left(L_Y^{\mathcal{C}}, \mathcal{E}_Y^{\mathcal{C}}\right) \tag{9}$$

The parameter $\mathcal{E}^{\mathcal{C}}$ has obtained by arbitrarily selecting the parameter like it is a co-prime of $M^{\mathcal{C}}$, in another expression

$$\mathbb{F}_{\mathcal{G}}\left(\mathcal{E}^{\mathcal{C}}, M^{\mathcal{C}}\right) = 1 \tag{10}$$

where $\mathbb{F}_{\mathcal{G}}(u, v)$ denotes the largest common factor function between u and v.

The decryption pair key of X and Y is described by $\left(L_X^{\mathcal{C}}, \mathcal{D}_X^{\mathcal{C}}\right)$ and $\left(L_Y^{\mathcal{C}}, \mathcal{D}_Y^{\mathcal{C}}\right)$. The $\mathcal{D}^{\mathcal{C}}$property is evaluated as follows:

$$\mathcal{D}^{\mathcal{C}} = \left(\mathcal{E}^{\mathcal{C}}\right)^{-1} \left| L^{\mathcal{C}} \right| \tag{11}$$

Let $\mathbb{E}_{\mathrm{U}}$ indicate the encrypted U message. The encryption process is as follows

$$\mathbb{E}_{\mathrm{U}} = \mathrm{V}^{\mathcal{E}^c} |\mathrm{L}^c| \tag{12}$$

The CRSA decryption process is expressed on $\mathcal{Y}$ encrypted message as

$$\mathbb{D}_{\mathrm{V}} = \mathrm{V}^{\mathcal{D}^c} |\mathrm{L}^c| \tag{13}$$

(d) Proof of commutative RSA model:

If the U message is encrypted with X and then encrypted with Y, the commutative RSA can be demonstrated by the SVC model. As for the encryption performed with Y, if it is encrypted at X, the message result is the same and can be expressed as follows:

$$\mathbb{E}^Y\left(\mathbb{E}_U^X\right) \equiv \mathbb{E}^X\left(\mathbb{E}_U^Y\right) \tag{14}$$

$$\mathbb{E}^Y\left(U^{\mathcal{E}_X^{\mathcal{C}}}\left|L_X^{\mathcal{C}}\right|\right) \equiv \mathbb{E}^X\left(U^{\mathcal{E}_Y^{\mathcal{C}}}\left|L_Y^{\mathcal{C}}\right|\right) \tag{15}$$

$$U^{(\mathcal{E}_X^{\mathcal{C}} \times \mathcal{E}_Y^{\mathcal{C}})}\left|L_X^{\mathcal{C}}\right| = U^{(\mathcal{E}_Y^{\mathcal{C}} \times \mathcal{E}_X^{\mathcal{C}})}\left|L_Y^{\mathcal{C}}\right| \tag{16}$$

As $L_X^{\mathcal{C}} = L_Y^{\mathcal{C}}$, it can be said that

$$U^{(\mathcal{E}_X^{\mathcal{C}} \times \mathcal{E}_Y^{\mathcal{C}})}\left|L_X^{\mathcal{C}}\right| = U^{(\mathcal{E}_Y^{\mathcal{C}} \times \mathcal{E}_X^{\mathcal{C}})}\left|L_X^{\mathcal{C}}\right| \tag{17}$$

and therefore,

$$\mathbb{E}^Y\left(\mathbb{E}_U^X\right) \equiv \mathbb{E}^X\left(\mathbb{E}_U^Y\right) \tag{18}$$

Each vehicle computes its public and private key using the proposed commutative RSA algorithm. Hop-based communication is adopted for data transmission among vehicles. Each vehicle encrypts the data using its own public key. The receiver performs decryption operations based on the number of times it is encrypted using its commutative keys of participating vehicles. The proposed model preserves data and user's privacy, and an intruder can be tracked using the user's commutative keys. First, once established the key management, the key management center will distribute two prime numbers A and B to all VANETs which are the same. Then, it will calculate L and M at each VANET node. Based on these two, each vehicular node will compute the encryption and decryption keys. Second, once established the key exchange and once all the vehicles do their encryption and decryption keys, they will inform the key management that it is over. For example (Figure 6):

1. Key setup:
   (a) The same values of A and B are considered in all VANETs distributed by the key management center.
   (b) L and M are calculated at each VANET node.

(c) Using random number generator encryption parameter E and decryption parameters D.

2. Key exchange:
   (a) Vehicle 1 is the source, and vehicle 4 is the destination.
   (b) Vehicle 4 will get decryption keys of vehicle 1, 2, and 3 (Vehicle 1 (1962914509, 1389794659), Vehicle 2 (1962914509,1608356723), Vehicle 3 (1962914509,1057410797)).
3. Secure data exchange (no original data are exposed/revealed):
   (a) Vehicle 1 will encrypt the data and send them to 2.
   (b) Vehicle 2 will encrypt data and send them to 3.
   (c) Vehicle 3 will encrypt the data and send them to 4.
   (d) Vehicle 4 will decrypt the data using keys of vehicles 3, 2, and 1 to get the original data.

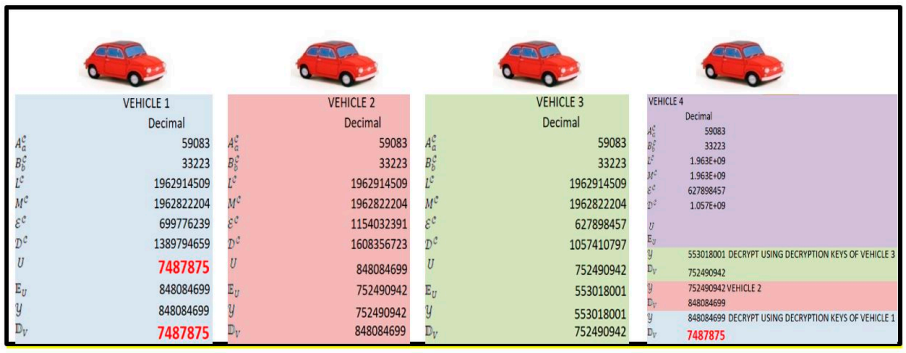

Figure 6. Example for CRSA.

In the normal RSA or Elliptical Curve Cryptography (ECC) [48], when you encrypt encrypted data again, data get corrupted. Therefore, on decryption, the data cannot be recovered. Therefore, in our mechanism, the user does not need to decrypt the data; the user can just encrypt using his key and forward it. The normal RSA implementation might not be very fruitful, and it remains unexplored even with recent and optimized encryption techniques. Hence, approaches like commutative characteristics, which means that the order in which encryption takes place does not affect the decryption process if it is done in the same way and avoids security breaching, can be implemented. The unique characteristic of commutative RSA cryptosystem is that it can facilitate the reorder decryption which is unique and effective itself. On the other hand, in most existing approaches, the public key cryptosystems employ a key exchange approach that ultimately causes the increase in computational overheads for key exchange, and alternatively, in individual transceiver, the encryption and decryption are a must, and thus somewhere, the efficiency as well as security would be compromised. Therefore, the consideration of commutative RSA (CRSA) might be an optimum solution for accomplishing an efficient and most secure communication for multi-channel V2V vehicular ad hoc smart infotainment applications.

(e) Computation of contention window:

To reduce the overhead probability between contending V vehicles considering security provisioning, contention window $\mathcal{A}$ is computed (example of contention window: a vehicle that wants to transmit a packet must first request a channel) [37]. Indeed, there is a tradeoff between collision probability and overhead of MAC protocol that is influenced by $\mathcal{A}$ (i.e., decreasing the $\mathcal{A}$ value increases the probability of the collision, in the cost of MAC lower overhead (lower MAC overhead: overhead incurred in defining contention window size)) and vice versa. However, each vehicle chooses some equal back-off time. However, the higher the probability of a collision, the higher the probability of a first collision because the number of vehicles involved decreases. (For example, firstly, 10 vehicles contend, and out of those, 5 get contention, so the collision likelihood is higher (20%). Then,

only the remaining 5 vehicles contend for the channel. Therefore, the likelihood of collision comes down.)

Let $\mathcal{L}_u$ be the probability of the first collision. Consider constraint $\mathcal{L}_u \leq \epsilon L$, where ϵL is the tradeoff between collision probability and management overhead to determine $\mathcal{A}$ contention window. For r vehicles in the window contention stage, $\mathcal{L}_u$ is evaluated as a function of $\mathcal{A}$. If there is no loss, consider the arbitrary back-off time of r vehicles (arbitrary back-off time of r vehicles is the random time selected by a set of r vehicles for contention (that is, r number of vehicles waiting for a while for channel access after detection of the first collision)) are arranged as $g_1 \leq g_2 \leq \cdots \leq g_r$. ($g_r$ is the random backoff time of each participating user in channel contention; r is the participation number of vehicles in the network. The first vehicle has the least waiting time, and the last vehicle has the maximum waiting time). Suppose r vehicles/devices in the contention stage; the probability of the 1st collision is shown as follows:

$$\mathcal{L}_u^{(r)} = \sum_{y=2}^{r} \mathbb{L}(y \; vehicles/device \; collide) = \sum_{y=2}^{r} \sum_{x=0}^{\mathcal{A}-2} U_r^y \left(\frac{1}{\mathcal{A}}\right)^y \left(\frac{\mathcal{A}-x-1}{\mathcal{A}}\right)^{r-y} \tag{19}$$

Each component in the double heaps shows the probability of a collision if y vehicles choose the same correction value for x. However, the probability of the first collision is computed as follows:

$$\mathcal{L}_u = \sum_{r=2}^{R} \mathcal{L}_u^{(r)} * \mathbb{L}\{r \; vehicle/device \; contend\} \tag{20}$$

where $\mathbb{L}\{r \; vehicle/device \; contend\}$ are the possibility of participating in the vehicles r in the contention stage and the Equation (19) is used to calculate $\mathcal{L}_u^{(r)}$. To rate $\mathcal{L}_u$, we derive $\mathbb{L}\{r \; vehicle/device \; contend\}$. If we have access to one channel T_x and all channels T_x^Soccupied, we can prove that x vehicle will participate in the contention. The probabilities of this scenario are expressed as:

$$\mathcal{L}_S^{(x)} = \mathbb{L}\left\{ \begin{array}{c} 1 \; channel \; at \; T_x^s \; is \; accessible \; and \\ all \; channels \; at \; T_x \; occupied \end{array} \right\} = \left(\prod_{y \epsilon T_x} \bar{l}_{xy}\right)\left(1 - \prod_{y \epsilon T_x^s} \bar{l}_{xy}\right) \tag{21}$$

The probability of the scenario in which the r vehicles users in the contention phase (contention phase is the period of the request of a channel for data transmission) is

$$\mathbb{L}\{ \; vehicle/device \; r \; contend\} = \sum_{k=1}^{U_R^r} \prod_{x \in \wedge_k} \mathcal{L}_S^{(x)} \prod_{x \in \wedge_R \backslash \wedge_t} \mathcal{L}_S^{(x)} \tag{22}$$

$\wedge_R$ is the group of all vehicles R ($\{1, 2, \ldots; R\}$), $\wedge_k$ is a particular group of r users. Output substitution of Equation (22) into Equation (20); $\mathcal{L}_u$ can be calculated. Nevertheless, it becomes possible to define $\mathcal{A}$ as

$$\mathcal{A} = \min\{\mathcal{A} | \mathcal{L}_u(\mathcal{A}) \leq \epsilon L\} \tag{23}$$

where, $\mathcal{L}_u$ in Equation (20) denotes a function of $\mathcal{A}$.

(f) Computation of Mac overhead:

Equation (23) can be used to model the overhead mean of MAC protocol. Let us consider h as the average value of the back-off parameters considering the security/safety selected by vehicles. Thus, $h = \frac{(\mathcal{A}-1)}{2}$, where the back-off value is determined uniformly between $\mathcal{A} - 1$ and 0 periods. Average overhead is calculated as follows:

$$\mathcal{D}(\mathcal{A}) = \frac{[\mathcal{A}-1]\varphi/2 + s_{CTS} + s_{RTS} + 3s_{SIFS} + s_{SYNC} + s_{SEN}}{S_{\mathcal{I}}} \tag{24}$$

where s_{CTS}, s_{RTS} and s_{SIFS} are the time corresponding of Request to Send (RTS), Clear to Send (CTS), and Short inter-frame space ($SIFS$) packets; s_{SYNC} is the synchronization of size packets; s_{SEN} is the sensing time; $S_{\mathcal{I}}$ is the time cycle, and φ is the one back-off param of corresponding time. The $\mathcal{D}$. overhead depends on the results of channel allocation. Thus, $\mathcal{D}$ is updated in flow diagram 2 based on the current channel assigned. Our PECA minimizes collision and maximizes system throughput, and provisioning security to S-PECA does not incur much overhead as proved in the next section experimentally.

4. Results

The experiments are conducted on a Windows 10 operating system, 64-bit I-5 quad-core processor with 32 GB RAM and Dedicated 4 GB NVidia CUDA GPU card. The SIMITS [39] simulator tool is used for experimental evaluation. The proposed PECA, $S-PECA$, and existing ENCCMA and $S-ENCCMA$ algorithms are written in C# object-oriented programing language using Visual studio framework 4.5, 2012. The PECA; $S-PECA$; $S-ENCCMA$; and city, highway, and rural radio propagating environment model (ours) are incorporated into the SIMITS tool. Experiments are conducted to evaluate the performance of $S-PECA$ over $S-ENCCMA$ in terms of throughput achieved, successful packet transmission, and packet collision. The experiments are conducted considering different environments such as city, highway, and rural [49–51].

For simulating and modeling the CHR environmental conditions, we considered the parameters presented in [52] (Table 3). Table 4 illustrates the evaluation simulation parameters.

Table 3. Channel parameters [52].

Environment	City	Highway	Rural
Path loss	1.61	1.85	1.79
Shadowing deviation	3.4	3.2	3.3

Table 4. Simulation parameters considered.

Parameters	Network	MAC	Modulation Scheme	Mobility	Bandwidth	Frequency Channels	Vehicles	Environment
Value	30 m ∗ 30 m	ENCCMA, S-ENCCMA, PECA andS-PECA	QAM-64	20 cycle per frame	27 Mbps	7	20	City, Highway, & Rural

(a) Throughput

The experiment was evaluated to assess the productivity performance of the proposed method with the state-of-the-art mechanisms and to assess overheads for providing security/safety to VANET. Firstly, we experiment to assess the throughput of PECA and ENCCMA considering the 20 vehicles in city, highway, and rural environments indicated in Figures 7–9, respectively. The experimental outcome shows that PECA improves throughput by 5.23%, 16.65%, and 37.97%, compared to ENCCMA, respectively in city, highway, and rural environments. An average throughput increased 19.95% by PECA compared to ENCCMA considering varied environmental models. Secondly, we evaluated $S-PECA$ and $S-ENCCMA$ by running the experiment on 20 vehicles used in city, highway, and rural environments, shown in Figures 7–9, considering security scheme. The experimental outcome shows that $S-PECA$ improves throughput by 13.22%, 45.54%, and 25.31% over $S-ENCCMA$ in city, highway, and rural environments. Considering the different environmental models, the average throughput increase of 28.02% is improved in $S-PECA$ compared to $S-ENCCMA$. The overall result shows that when a security scheme is added to PECA and ENCCMA, the model incurs an average throughput overhead of 7.2% and 15.91%, respectively, when provisioning security considering the varied environment model. Overall results show the proposed PECA model performs much better than the

existing ENCCMA significantly in terms of throughput performance when provisioning security to it.

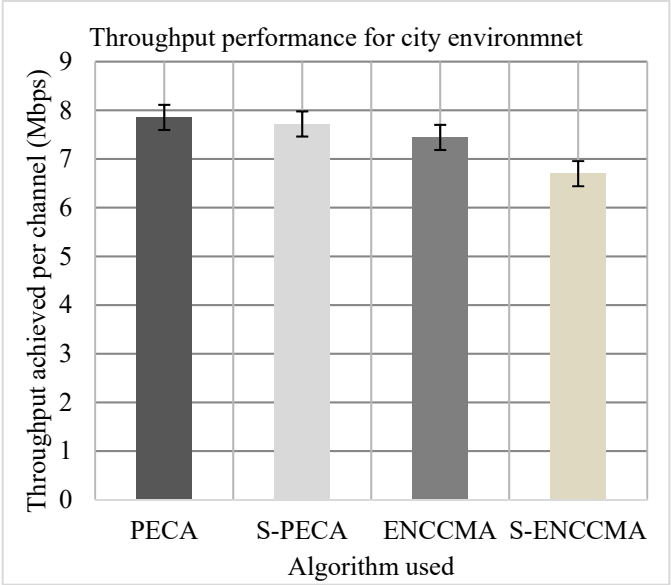

Figure 7. Throughput performance for the city environment.

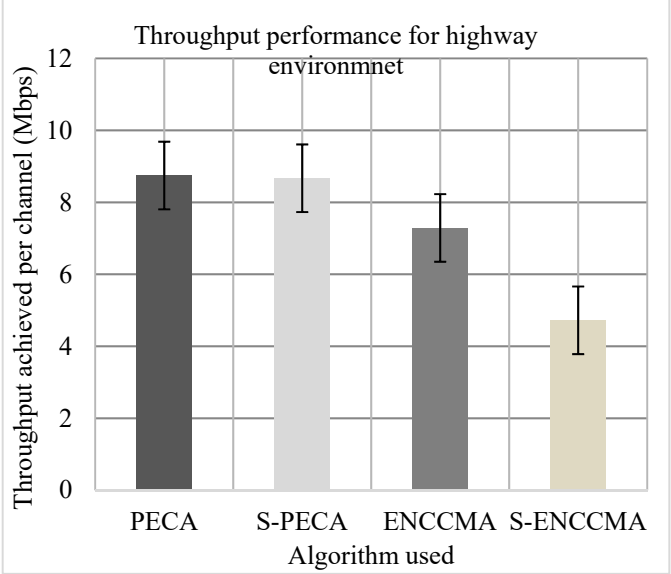

Figure 8. Throughput performance for highway environment.

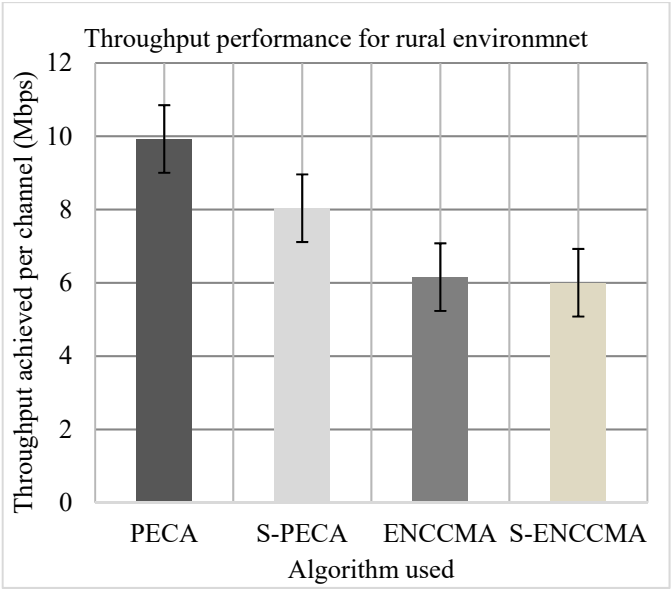

Figure 9. Throughput performance for the rural environment.

(b) Collision

The experiment was performed to assess the collision of the proposed method with the existing method and to assess the overhead that happened in provisioning safety to VANET. First, the experiment evaluated the collision performance of PECA and ENCCMA using 20 vehicles for the CHR environment as shown in Figures 10–12, respectively. The experimental outcome shows that PECA reduces collision by 44.44%, 35.29%, and 74.13% compared to ENCCMA in city, highway, and rural environments. The average collision reduction of 51.31% is performed by PECA compared to ENCCMA considering varied environmental models. Secondly, the experiment is evaluated the collision of $S-PECA$ and $S-ENCCMA$, respectively, considering 20 vehicles in the city, highway, and rural environments, shown in Figures 10–12, considering security scheme. The experimental outcome shows that $S-PECA$ reduces collision by 46.15%, 63.41%, and 61.9% over $S-ENCCMA$, respectively, in city, highway, and rural environments. The average collision reduction of 57.15% is performed in $S-PECA$ compared to $S-ENCCMA$. considering varied environmental models. The overall result shows that when a security scheme is added to PECA and ENCCMA, the model incurs an average collision overhead of 35.07% and 15.91%, respectively, when provisioning security considering the varied environment model. The overall result obtained shows the proposed PECA model performs much better than the existing ENCCMA significantly in terms of collision performance when provisioning security to it.

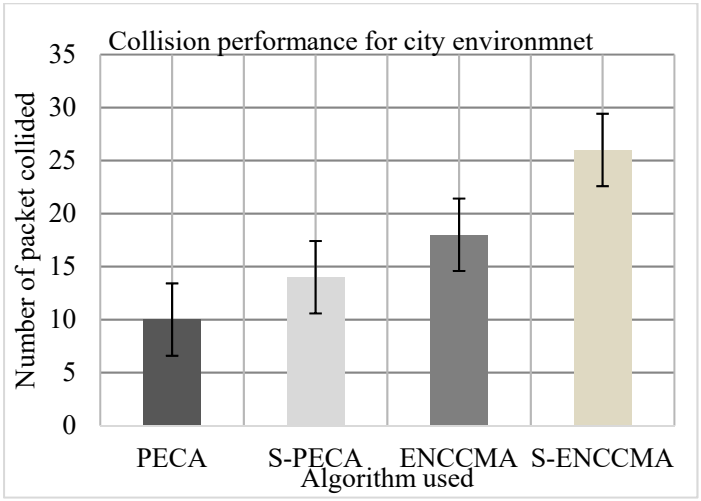

Figure 10. Collision performance for the city environment.

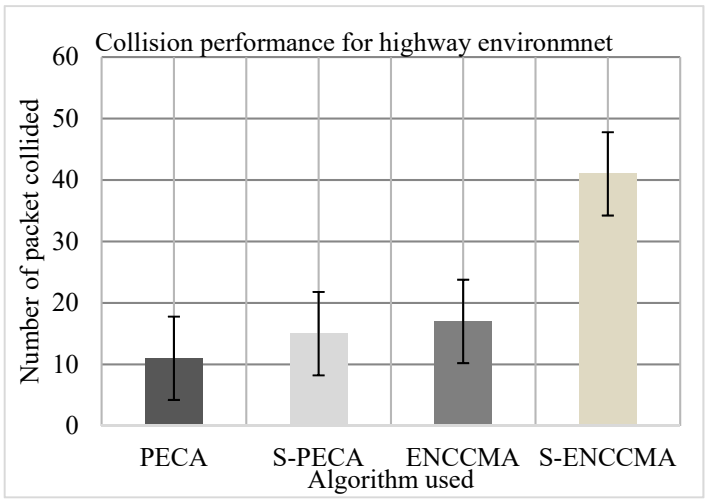

Figure 11. Collision performance for highway environment.

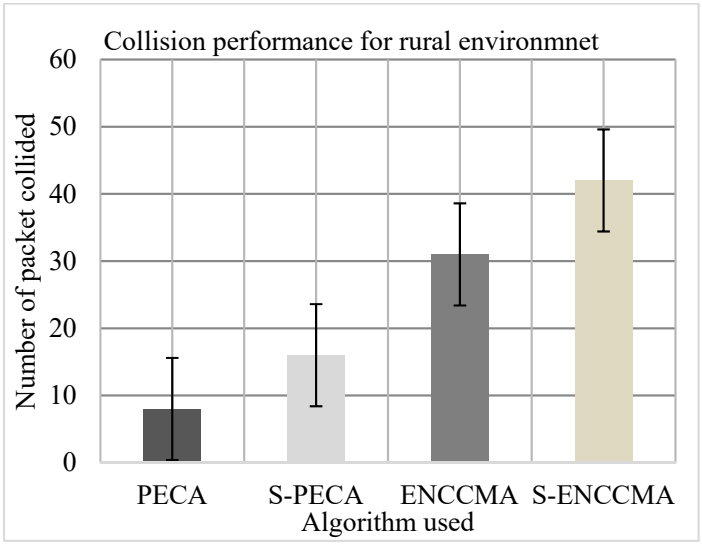

Figure 12. Collision performance for the rural environment.

(c) Performance of successful data transmission

Experiments were conducted to evaluate the packet transfer of the proposed method compared to the existing method, and the overhead of VANET security configuration was also evaluated. First, the experiment evaluated the successful transmission of PECA and ENCCMA using 20 vehicles in the various environments as we can see in Figures 13–15, respectively. The experimental outcome shows that PECA performed a successful transmission of packets by 5.0%, 9.52%, and 33.8%, respectively, compared to ENCCMA in city, highway, and rural environments. The average improvement of the successful transmission is 21.66% achieved by PECA compared to ENCCMA considering varied environmental models. Secondly, the experiment was conducted to perform the packet transfer performance of S − PECA and S − ENCCMA considering 20 vehicles for C.H.R environments as shown in Figures 13–15, respectively, considering security scheme. The experimental outcome shows that S − PECA improves successful packet transmission by 15.0%, 41.93%, and 24.13% over S − ENCCMA in city, highway, and rural environments. The average improvement of successful transmission is 27.02% achieved by S − PECA compared with S − ENCCMA considering varied environmental models. The overall result show that when a security scheme is added to PECA and ENCCMA, the model incurs an average successful packet transmission overhead of 6.63% and 17.97%, respectively, when provisioning security considering varied environment model. However, we can see the proposed PECA model performed much better than the existing ENCCMA, significantly in terms of successful transmission performance when provisioning security to it.

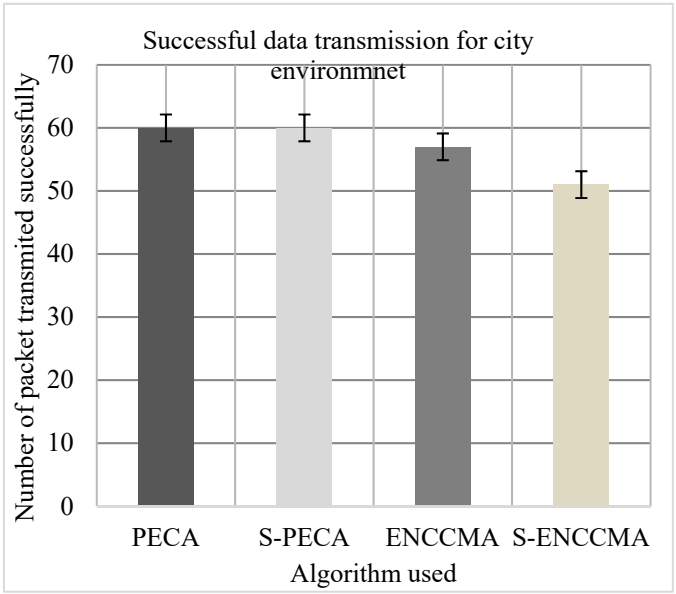

Figure 13. Successful transmission performance for city.

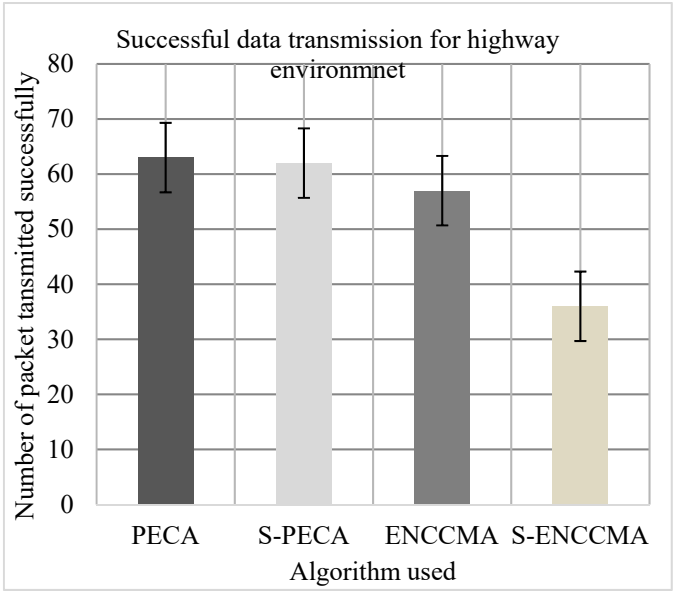

Figure 14. Successful transmission for highway.

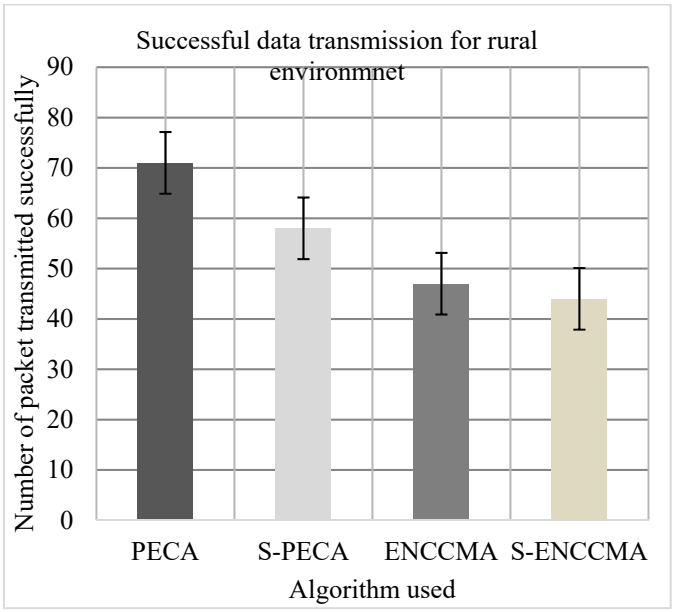

Figure 15. Successful transmission performance for rural.

5. State-of-the-Art Technology Comparison

Table 5 shows the comparison between S − PECA with the state-of-the-art technology. To improve the system efficiency, S − PECA supports distribute channel sharing mechanism in V2 V environments and helps the system to achieve maximum throughput and minimum overhead. The S − ENCCMA adopts the enhanced non-cooperative cognitive division multiple access (ENCCMA) [37] real-time MAC communication protocol. To provision real-time access, the ENCCMA combines Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), and Cognitive Radio (CR) techniques. The ENCCMA MAC protocol avoids signaling; this aids in enhancing the system's efficiency. However, ENCCMA did not consider message authentication and security for personal user information. Reference [53] evaluated the performance of transmission of packet data considering different environments. However, they did not consider the movement and the numbers of the vehicles. In [54], the author performed an experimental analysis that considers different speeds for collision performance evaluation. However, their model did

not consider experimental study under different environmental conditions such as city, highway, and rural and induced MAC protocol overhead [17]. Compared with the other models, our model presents a secure and efficient distributed design for channel allocation that maximizes the system throughput and reduces packet collision considering different environmental conditions. The list of the abbreviation and acronyms used in the text are presented in Table 6.

Table 5. State of-art-techniques comparison.

	PECA/ S − PECA/ S − ENCCMA	**ENCCMA**	**MS − ALOHA**	**SLOP**	**EDF − CSMA**
Environment	C.H.R	Flowing vehicles freely	Highway and Urban	driver intelligent	NA
Algorithm	NSCA/SCA	(NCC − FDMA − TDMA)	MS − ALOHA	Wave − Slotted aloha	EDF − CSMA
Vehicle varied Density	Yes	No	No	No	No
Simulator used	SIMITS	SIMITS	VISSIM	YES (NA)	NS − 3
MAC USED	802.11p MAC	802.11p MAC	802.11p MAC	802.11p MAC	802.11p MAC
Mobility	Yes	Yes	Yes	Yes	Yes
Channel sharing available	Yes	Yes	No	No	No
Reference	(Ours)	[37]	[53]	[54]	[17]

Table 6. Abbreviations and Acronyms.

Acronyms	**Definition**
VANET	Vehicular Ad hoc Network
S − PECA	Secure Performance Enriched Channel Allocation
S − ENCCMA	Secure Non-Cooperative Cognitive Division Multiple Access
TDMA	Time Division Multiple Access
FDMA	Frequency Division Multiple Access
RSA	Rivest–Shamir–Adleman
CR	Cognitive Radio
V2V	Vehicle to Vehicle
V2I	Vehicle to Infrastructure
V2X	Vehicle to Everything
OBU	On Board Unit
RSU	Road-Side Unit
DSRC	dedicated short range communication
MAC	Medium Access Control
MANET	Mobile Ad hoc Network
FCC	Federal Communications Commission
ITS	Intelligent Transportation Systems
RFID	Radio-frequency identification
WAVE	Wireless Access in Vehicular Environment
GPS	Global Positioning System
LTE	Long-Term Evolution
V2N	Vehicle-to-Network
PLS	Physical Layer Security
IoV	Internet of Vehicles
CRL	Certificate Revocation List
RIS	reconfigurable intelligent surface
IoT	Internet of things
SVC	Secure VANET Communication
NSCA	Non-Shared Channel Allocation
ECC	Elliptical Curve Cryptography
CRSA	Commutative RSA
CHR	City, Highway, and Rural
MS-Aloha	Mobile Slotted Aloha
VISSIM	Verkehr In Stadten Simulationsmodell
EDF − CSMA	Earliest Deadline First based Carrier Sense Multiple Access

6. Conclusions

This work presented a secure MAC design for VANET. This model presented a commutative RSA-based channel allocation scheme on a shared channel network, namely S-PECA. The S-PECA model has overcome the key management and communication overhead issue of exiting third-party server and public-key cryptography schemes. Experiments are conducted to evaluate the overhead incurred in provisioning security to S-PECA and S-ENCCMA. The S-PECA and S-ENCCMA protocols incur an average throughput overhead of 7.2% and 15.91%, average collision overhead of 35.07% and 38.91%, and average success packet transmission overhead of 6.63% and 17.97% when security is provisioned to S-PECA and ENCCMA, respectively, considering the different environmental conditions. The outcome shows that overhead incurred by S-PECA is much lower when compared to S-ENCCMA in terms of throughput, collision, and successful packet transmission considering varied environmental models. The overall outcome shows S-PECA minimizes collision and maximizes system throughput considering different radio propagation environments when compared to state-of-the-art techniques. In future work, we would consider performance evaluation under various modulation schemes and consider designing a new security mechanism for VANET.

Author Contributions: M.A.A.-A. and A.A.A.-A. contributed to the main idea and the methodology of the research. M.A.A.-A. designed the experiment, performed the simulations, and wrote the original manuscript. A.A.A.-A., R.F., K.-H.K. and Y.-S.L. contributed significantly to improving the technical and grammatical contents of the manuscript. A.A.A.-A., B.-G.L., S.-G.L. and H.-J.L. reviewed the manuscript and provided valuable suggestions to further refine it. Supervision, H.-J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was a part of the project titled 'Marine digital AtoN information management and service system development (1/5) (20210650)', funded by the Ministry of Oceans and Fisheries, Korea.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

References

1. Issam, W.; Damaj, D.; Serhal, K.; Lama, A.; Rached, H.; Zantout, N.; Mouftah, H.T. Connected and Autonomous Electric Vehicles: Quality of Experience survey and taxonomy. *Veh. Commun.* **2021**, *28*, 100312.
2. Ros, F.J.; Ruiz, P.M.; Stojmenovic, I. Acknowledgment-based broadcast protocol for reliable and efficient data dissemination in vehicular ad-hoc networks. *IEEE Trans. Mob. Comput.* **2012**, *11*, 33–46. [CrossRef]
3. Ahmed, A.; Rasheed, H.; Liyanage, M. Millimeter-Wave Channel Modeling in a Vehicular Ad-Hoc Network Using Bose–Chaudhuri–Hocquenghem (BCH) Code. *Electronics* **2021**, *10*, 992. [CrossRef]
4. Azees, M.; Vijayakumar, P.; Deborah, L.J. Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intell. Transp. Syst.* **2016**, *10*, 379–388. [CrossRef]
5. Dedicated Short Range Communications (DSRC). Available online: http://grouper.ieee.org/groups/scc32/dsrc/index.html (accessed on 1 July 2021).
6. Keyvan, A. Joint use of DSRC and C-V2X for V2X communications in the 5.9 GHz ITS band. *IET Intell. Transp. Syst.* **2021**, *15*, 213–224.
7. Petit, J.; Schaub, F.; Feiri, M.; Kargl, F. Pseudonym Schemes in Vehicular Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 228–255. [CrossRef]
8. Kiela, K.; Barzdenas, V.; Jurgo, M.; Macaitis, V.; Rafanavicius, J.; Vasjanov, A.; Kladovscikov, L.; Navickas, R. Review of V2X–IoT Standards and Frameworks for ITS Applications. *Appl. Sci.* **2020**, *10*, 4314. [CrossRef]
9. Miao, L.; Virtusio, J.J.; Hua, K.-L. PC5-Based Cellular-V2X Evolution and Deployment. *Sensors* **2021**, *21*, 843. [CrossRef]
10. Mohammed, A.A.; Ahmed, A.A.; Lee, H.J. V2V communication modeling for environmental channel throughput and radio propagation. In Proceedings of the 8th IEEE International Conference on ICTC Convergence, Jeju Island, Korea, 18–20 October 2017; pp. 507–512.
11. Mohammed, A.A.; Ahmed, A.A.; Kang, Y.J.; Lee, H.J. Obstacles Effects on Signal Attenuation in Line of Sight for Different Environments in V2V. In Proceedings of the 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si, Gangwon-do, Korea, 11–14 February 2018; pp. 17–20.

12. ITS Standards Fact Sheets. In *Proceedings of the IEEE 1609—Family of Standards for Wireless Access in Vehicular Environments (WAVE)*; United States Department of Transportation: Washington, DC, USA, 2009.
13. Storck, C.R.; Duarte-Figueiredo, F. A Survey of 5G Technology Evolution, Standards, and Infrastructure Associated with Vehicle-to-Everything Communications by Internet of Vehicles. *IEEE Access* **2020**, *8*, 117593–117614. [CrossRef]
14. Mohammed, A.A.; Ahmed, A.A.; Lee, H.J. Performance Analysis for City, Highway and Rural Area in Vehicle-to-Vehicle Network. In Proceedings of the 8th IEEE International Conference on ICTC Convergence, Jeju Island, Korea, 17–19 October 2018.
15. Mohammed, A.A.; Ahmed, A.A.; Hind, R.; Lee, H.J. A Novel Throughput and Collision for City Environment in V2V Communication. In Proceedings of the 10th IEEE International Conference on ICTC Convergence, Jeju Island, Korea, 16–18 October 2019; pp. 1413–1415.
16. Mohammed, A.A.; Ahmed, A.A.; Lee, H.J. Comparison between DSRC and other Short-Range Wireless Communication Technologies. In Proceedings of the 2020 22nd International Conference on Advanced Communication Technology (ICACT) Phoenix Park, PyeongChang, Korea, 16–19 February 2020; pp. 1–5.
17. Chang, C.Y.; Yen, H.C.; Deng, D.J. V2V QoS Guaranteed Channel Access in IEEE 802.11p VANETs. *IEEE Trans. Veh. Technol.* **2015**, *13*, 5–17. [CrossRef]
18. EU Road Safety Policy Framework 2021–2030—Next steps towards "Vision Zero", European Commission, Brussels, 19.6.2019. Available online: https://ec.europa.eu/transport/sites/transport/files/legislation/swd20190283-roadsafety-vision-zero.pdf (accessed on 2 May 2021).
19. 40+ Corporations Working on Autonomous Vehicles, 16 December 2020. Available online: https://www.cbinsights.com/research/autonomous-driverless-vehicles-corporations-list/ (accessed on 6 May 2021).
20. IEEE Connected & Autonomous Vehicles. Available online: https://site.ieee.org/connected-vehicles/news/news/ (accessed on 4 June 2021).
21. Ho, T.M.; Tran, T.D.; Nguyen, T.T.; Kazmi, S.M.A.; Le, L.B.; Hong, C.S.; Hanzo, L. Next-generation wireless solutions for the smart factory, smart vehicles, the smart grid and smart cities. *arXiv* **2019**, arXiv:1907.10102.
22. Contreras-Castillo, J.; Zeadally, S.; Guerrero-Ibáñez, J. Internet of Vehicles: Architecture, Protocols, and Security. *IEEE Internet Things J.* **2018**, *5*, 3701–3709. [CrossRef]
23. Bharat, M.; Sree, K.S.; Kumar, T.M. Authentication solution for security attacks in VANETs. *Int. J. Adv. Res. Comput. Commun. Eng.* **2014**, *3*, 7661–7664.
24. Farash, M.S.; Turkanović, M.; Kumari, S.; Hölbl, M. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. *Ad Hoc Netw.* **2016**, *36*, 152–176. [CrossRef]
25. Li, H.; Lu, R.; Zhou, L.; Yang, B.; Shen, X. An efficient Merkletree- based authentication scheme for smart grid. *IEEE Syst. J.* **2014**, *8*, 655–663. [CrossRef]
26. Li, H.; Liu, D.; Dai, Y.; Luan, T.H. Engineering searchable encryption of mobile cloud networks: When QoE meets QoP. *IEEE Wirel. Commun.* **2015**, *22*, 74–80. [CrossRef]
27. Qu, F.; Wu, Z.; Wang, F.Y.; Cho, W. A security and privacy review of VANETs. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 2985–2996. [CrossRef]
28. He, D.; Zeadally, S.; Xu, B.; Huang, X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular adhoc networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]
29. Kafle, V.P.; Fukushima, Y.; Fujikawa, K.; Harai, H. ID-based communication framework in future networks. *Wirel. Pers. Commun.* **2016**, *86*, 1735–1750. [CrossRef] Personal
30. Zhou, A.; Li, J.; Sun, Q.; Fan, C.; Lei, T.; Yang, F. A security authentication method based on trust evaluation in VANETs. *EURASIP J. Wirel. Commun. Netw.* **2015**, *1*, 1. [CrossRef]
31. Li, W.; Song, H. ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 960–969. [CrossRef]
32. Wagan, A.A.; Jung, L.T. Security framework for low latency VANET applications. In Proceedings of the IEEE International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 3–5 June 2014; pp. 1–6.
33. Suresh, J.S.; Jongkun, L. A TPM-based architecture to secure VANET. *Indian J. Sci. Technol.* **2015**, *8*, 15. [CrossRef]
34. Rehman, A.; Hassan, M.F.B. Design Specification of Context Cognitive Trust Evaluation Model for V2V Communication in IoV. Emerging Trends in Intelligent Computing and Informatics, (IRICT 2019). *Adv. Intell. Syst. Comput.* **2019**.
35. Rajput, U.; Abbas, F.; Oh, H. A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET. *IEEE Access* **2016**, *4*, 7770–7784. [CrossRef]
36. Liu, Y.; Wang, Y.; Chang, G. Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm. *IEEE Trans. Intell. Transp. Syst.* **2017**, *99*, 1–10. [CrossRef]
37. Al-Absi, M.A.; Al-Absi, A.A.; Lee, H.J. Performance Enriching Channel Allocation Algorithm for Vehicle-to-Vehicle City, Highway and Rural Network. *Sensors* **2019**, *19*, 3283. [CrossRef]
38. Han, Y.; Ekici, E.; Kremo, H.; Altintas, O. Throughput-Efficient Channel Allocation Algorithms in Multi-Channel Cognitive Vehicular Networks. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 757–770. [CrossRef]
39. Manzano, M.; Espinosa, F.; Ángel, M.; Santos, B.; Vicente, A.G. Cognitive Self-Scheduled Mechanism for Access Control in Noisy Vehicular Ad Hoc Networks. Hindawi Publishing Corporation. *Math. Probl. Eng.* **2015**, *2015*, 354292. [CrossRef]

40. Kasana, R.; Kumar, S.; Kaiwartya, O.; Yan, W.; Cao, Y.; Abdullah, A. Location error resilient geographical routing for vehicular ad-hoc networks. *IET Intell. Transp. Syst.* **2017**, *11*, 450–458. [CrossRef]
41. Makarfi, A.U.; Rabie, K.M.; Kaiwartya, O.; Xingwang Li, X.; R. Kharel, R. Physical Layer Security in Vehicular Networks with Reconfigurable Intelligent Surfaces. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; pp. 1–6.
42. Hsiao, H.; Studer, A.; Chen, C.; Perrig, A.; Bai, F.; Bellur, B. Floodingresilient Broadcast Authentication for VANET. In Proceedings of the 17th Annual International Conference on Mobile Computing and Networking (MobiCom), Las Vegas, NV, USA, 19–23 September 2011; pp. 193–204.
43. Moayad, A.; Safa, O.; Ismaeel, A.R.; Yaser, J. An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Netw.* **2019**, *90*, 101842.
44. Balasubramanian, V.; Aloqaily, M.; Reisslein, M. An SDN architecture for time sensitive industrial IoT. *Comput. Netw.* **2021**, *186*, 107739. [CrossRef]
45. Ridhawi, I.A.; Otoum, S.; Aloqaily, M.; Jararweh, Y.; Baker, T. Providing secure and reliable communication for next generation networks in smart cities. *Sustain. Cities Soc.* **2020**, *56*, 102080. [CrossRef]
46. Wei, Z.; Yanjiang, Y.; Wu, Y.; Weng, J.; Deng, R.H. HIBS-KSharing: Hierarchical Identity-Based Signature Key Sharing for Automotive. *IEEE Access* **2017**, *5*, 16314–16323. [CrossRef]
47. Cui, J.; Zhang, J.; Zhong, H.; Xu, Y. SPACF: A Secure Privacy-preserving Authentication Scheme for VANET with Cuckoo Filter. *IEEE Trans. Veh. Technol.* **2017**, *66*, 10283–10295. [CrossRef]
48. TABF Editorial Board; Huang, H.C.C. *Basic Knowledge on FinTech*; Hyweb Technology Co. Ltd.: Zhubei City, Taiwan, 2020.
49. Al-Absi, M.A.; Al-Absi, A.A.; Lee, H.J. Varied density of vehicles under city, highway and rural environments in V2V communication. *Int. J. Sens. Netw.* **2020**, *33*, 148–158. [CrossRef]
50. Mohammed, A.A.; Ahmed, A.A.; Kim, T.; Lee, H.J. An Environmental Channel Throughput and Radio Propagation Modeling for Vehicle-to-Vehicle Communication. *Int. J. Distrib. Sens. Netw.* **2018**, *14*, 1–10.
51. Al-Absi, M.A.; Al-Absi, A.A.; Sain, M.; Lee, H. Moving Ad Hoc Networks—A Comparative Study. *Sustainability* **2021**, *13*, 6187. [CrossRef]
52. Bilgin, B.E.; Gungor, V.C. Performance Comparison of IEEE 802.11p and IEEE 802.11b for Vehicle-to-Vehicle Communications in Highway, Rural, and Urban Areas. *Int. J. Veh. Technol.* **2013**, *2013*, 971684. [CrossRef]
53. Bazzi, A.; Zanella, A.; Masini, B.M. An OFDMA-Based MAC Protocol for Next-Generation VANETs. *IEEE Trans. Veh. Technol.* **2015**, *64*, 4088–4100. [CrossRef]
54. Ferreira, N.F.G.C.; Fonseca, J.A.G. Improving Safety Message Delivery through RSU's Coordination in Vehicular Networks. In Proceedings of the 2015 IEEE World Conference on Factory Communication Systems (WFCS), Palma de Mallorca, Spain, 27–29 May 2015; pp. 1–8.