electronics

Article

A Novel Cross-Layer V2V Architecture for Direction-Aware Cooperative Collision Avoidance

Shahab Haider [1], Ziaul Haq Abbas [2], Ghulam Abbas [1,3], Muhammad Waqas [3,4], Shanshan Tu [4,5,*] and Wei Zhao [6]

[1] Telecommunications and Networking (TeleCoN) Research Lab, GIK Institute of Engineering Sciences and Technology, Topi 23640, Pakistan; shahab@giki.edu.pk (S.H.); abbasg@giki.edu.pk (G.A.)
[2] Faculty of Electrical Engineering, GIK Institute of Engineering Sciences and Technology, Topi 23640, Pakistan; ziaul.h.abbas@giki.edu.pk
[3] Faculty of Computer Science and Engineering, GIK Institute of Engineering Sciences and Technology, Topi 23640, Pakistan; engr.waqas2079@gmail.com
[4] Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China
[5] Engineering Research Center of Intelligent Perception and Autonomous Control, Ministry of Education, Beijing 100124, China
[6] Beijing Electro-Mechanical Engineering Institute, Beijing 100074, China; qiuhuabb@163.com
* Correspondence: sstu@bjut.edu.cn

Received: 25 May 2020; Accepted: 5 July 2020; Published: 8 July 2020

Abstract: The death toll due to highway crashes is increasing at an alarming rate across the globe. Vehicular Ad Hoc Networks (VANETs) have emerged as a promising solution to prevent crashes by enabling collision avoidance applications. However, a robust and stable collision avoidance application is a cross-layer problem that must address a number of key challenges across all layers of a VANET communication architecture. This paper presents and evaluates a novel VANET protocol suite, named Direction-Aware Vehicular Collision Avoidance (DVCA), which covers application, security services, network, and link layers. DVCA is a vehicle-to-vehicle communication architecture that provides enhanced collision probability computation and adaptive preventive measures for cooperative collision avoidance on bi-directional highways. Moreover, DVCA enables secure, in-time, and reliable dissemination of warning messages, which provides adequate time for vehicles to prevent collisions. Simulation and analytical results demonstrate reasonable reduction in collisions by DVCA, as compared with eminent VANET communication architectures.

Keywords: intelligent transportation systems; collision avoidance; vehicle-to-vehicle communication; VANET architecture

1. Introduction

1.1. Motivation and Objectives

Vehicular accidents (hereinafter collisions) on conventional highways have been increasing at an alarming rate. Each year, an estimated 1.35 million deaths and 20–50 million injuries occur around the world due to collisions [1,2]. To this end, Intelligent Transportation Systems (ITSs) introduce innovative techniques to enable safe traffic environments [3]. Vehicular Ad Hoc Networks (VANETs) are the primary enablers of ITSs for transforming ordinary vehicles into intelligent and communicating entities (hereinafter nodes). VANETs connect high-speed nodes for sharing information pertaining to their speed, direction, and position in a highly dynamic network topology to enable various ITS applications, such as infotainment, route identification, and Cooperative Collision Avoidance (CCA) [4,5]. A CCA can mitigate collisions by enabling nodes to foresee hazardous events through the exchange of warning messages [6]. This provides nodes with reasonable reaction time for applying preventive measures, such as the reduction of speed.

The connectivity among nodes in VANETs is achieved through two communication models, namely, Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V). Nodes in a V2V model communicate directly with each other, whereas roadside units are employed for communication in a V2I model to route packets to other nodes or to a base station [6,7]. The V2I model exhibits increased costs of deployment and maintenance of infrastructure as compared to the V2V model [8–10]. Both the communication models also often employ clustering to group similar nodes and manage communications efficiently through Cluster Heads (CHs) [11,12].

VANET communication architectures [13], such as Wireless Access in Vehicular Environments (WAVE) [14], comprise a protocol suite with multiple layers. These include application, security services, network, Media Access Control (MAC) and physical layers. The application layer is responsible for identification of possible collisions and specification of preventive measures, which are disseminated in the network in the form of warning messages. The security service layer is responsible for securing the warning messages. The network layer routes warning messages to destination nodes on optimal paths to reduce transmission delays and packet losses. Finally, the MAC layer seeks to enhance the utilization of shared channels. A VANET communication architecture can be utilized for developing various ITS applications, such as infotainment, route identification, and CCA.

However, for efficient collision avoidance in a CCA application, a number of challenges must be addressed across all layers of a VANET communication architecture. The existing VANET architectures [13,14] do not take into account the direction of nodes, which is a critical parameter for collision avoidance on bi-directional highways. This results in inaccurate collision probability computations at the application layer [15]. Additionally, the existing application layer protocols rely on fixed decelerations as preventive measures, which adversely impact their performance [15]. At security services layer, the existing architectures compromise the confidentiality of warning messages, in that they transmit warning messages as plaintext and exhibit high computational and communication overheads [16]. Moreover, the capability to cater for frequent topological changes on bi-directional highways while routing warning messages is also found lacking in the existing VANET architectures [17]. Furthermore, un-prioritized transmission of warning message at MAC layer is yet another critical limitation in the existing VANET architectures [18].

1.2. Our Contributions

In [15–18], we have proposed direction-aware V2V protocols for each layer of the VANET architecture to overcome the aforementioned challenges. These include:

- An application layer protocol, called Probabilistic-Direction Aware Cooperative Collision Avoidance (P-DACCA) [15], which is a pioneering CCA application for bi-directional highways to not only mitigate inter-cluster and intra-cluster collisions, but also provide enhanced cluster stability, and minimize communication overhead and transmission latency,
- A security service layer protocol, called Light-Weight Encryption-Enabled Conditional Privacy Preserving Authentication (LWE-CPPA) [16], which preserves nodes' privacy, authenticates messages, and provides protection against blackhole attacks to enable secure transmission of warning messages,
- A network layer protocol, called Direction Aware Best Forwarder Selection (DABFS) [17] that takes into account directions and relative positions of nodes to provide reliable and timely delivery of warning messages, and
- A MAC layer protocol, called Priority-Based Direction-Aware Media Access Control (PDMAC) [18] that performs intra-cluster as well as inter-cluster clock synchronization, and introduces a three-tier priority assignment technique to enhance channel utilization and

warning messages delivery.

Each of our previously proposed protocols [15–18] has been demonstrated to outperform eminent existing protocols of the corresponding layer. However, performance evaluations in [15–18] consider the performance metrics of the corresponding layer only. For generating simulation results of a particular protocol, standard protocols were used at all other layers.

This paper consolidates our previous work [15–18] into a framework of a suite of protocols, named Direction-Aware Vehicular Collision Avoidance (DVCA). DVCA, thus, constitutes a novel cross-layer V2V communication architecture, depicted in Figure 1, for direction-aware cooperative collision avoidance, and harnesses the strengths and benefits of our previously proposed protocols [15–18]. We evaluate the performance of DVCA in comparison with similar existing VANET communication architectures for collision avoidance. To that end, the competing protocol suites are treated as black-boxes with similar inputs and outputs to evaluate the cumulative effect of each framework. Through simulation and analytical results, we demonstrate that DVCA is able to reasonably reduce collisions on bi-directional highways due its direction-aware collision probability computation, adaptive preventive measures, and efficient and secure dissemination of warning messages.

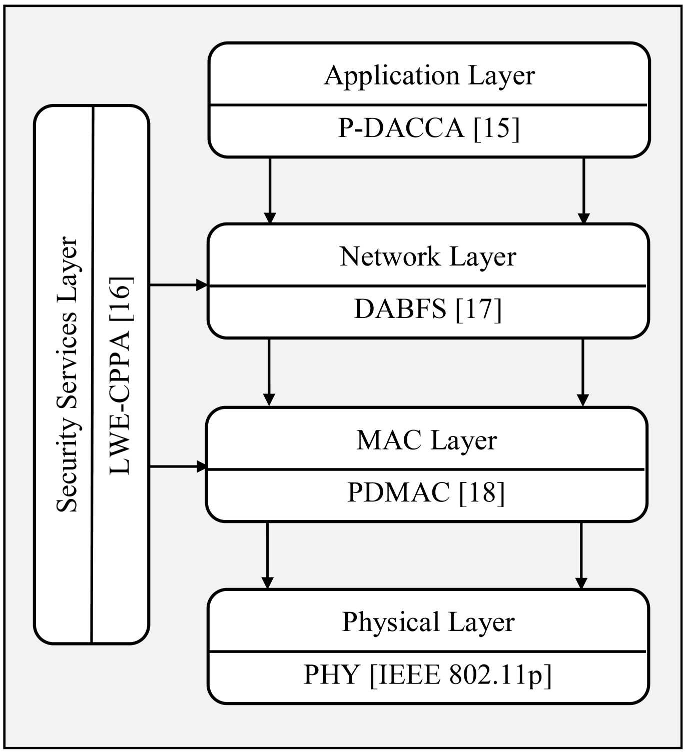


Figure 1. The proposed Direction-Aware Vehicular Collision Avoidance (DVCA) architecture.

1.3. Paper Organization

In the remainder of this paper, Section 2 presents the related work on VANET communication architectures. Section 3 presents the proposed DVCA architecture. Section 4 presents performance evaluation, and Section 5 concludes the paper and provides future research directions.

2. Related Work

A VANET communication architecture consists of multiple layers, including application, security services, network, MAC, and physical layers. For cooperative collision avoidance, the application layer performs nodes' clustering, predicts possible collisions, and specifies preventive measures. Warning messages are generated at this layer to intimate other nodes regarding hazardous events and transmitted by employing the services of the lower layers [19]. Secure transmission of warning messages remains critical [20], as malicious activities performed on warning messages may cause collisions at a large scale. The security services layer is responsible for ensuring the security. Since in-time and reliable delivery of these time-sensitive messages also remains important, the network layer routes warning messages to destination nodes on optimal paths to reduce transmission delays and packet losses. MAC layer seeks to enhance the utilization of shared channels and physical layer puts bits on the communication media for transmission. Since each layer has its own significance, effective collision avoidance does not remain restricted to a single layer and, hence, is a cross-layer issue [21]. This section reviews eminent VANET architectures in the existing literature.

IEEE standardized 1609 protocol stack, namely, Wireless Access in Vehicular Environment (WAVE), provides a layered architecture for handling diverse issues related to all VANET communication layers. The protocol suite includes 1609.1 through 1609.6 standards for the application layer through physical layer. WAVE has two modes, namely, safety and non-safety modes and it uses dedicated 5.9 GHz frequency band for communication [22]. Continuous Air Interface for Long to Medium Range (CALM) [23] is the International Standards Organization (ISO) proposal for continuous inter-node communication in VANETs through V2V as well as V2I models. The concept aims at establishing communication among different kinds of devices, such as On-Board Units (OBUs) and Road Side Units (RSUs). CALM interface manager, CALM network manager, and CALM application manager constitute the management entity in CALM. Car-to-Car Communication Consortium (C2C-CC) [24] enables V2V and V2I communications. C2C-CC architecture introduces a C2CNet protocol at network layer that supports both safety and non-safety applications in a multi-hop network.

The work in [25] proposes a heterogeneous communication architecture for VANETs, where a node can connect through WiFi, WAVE, or a Fourth Generation (4G) Long Term Evolution (LTE) interface. The interfaces can be switched to achieve the best services at a particular time. The authors in [26] propose a secure distributed VANET architecture to build an efficient cloud that can be exploited to provide different services, such as parking area management, collision avoidance, traffic congestion avoidance, etc. A similar secure architecture is proposed in [27]. The work in [28] proposes a two-tier VANET architecture, called Mobile Infrastructure based VANET Architecture for Urban Environment (MI-VANET). This architecture takes buses as backbone on the first tier for messages transmission, whereas the ordinary nodes constitute the second tier. Mobile Infrastructure Registering (MIRG) and Mobile Infrastructure Routing (MIRT) algorithms perform nodes registration and buses density computation, respectively.

The authors in [29] propose a three-tier secure Internet of Vehicle (IoV) architecture that employs Reputation-Based Vehicle-Assisted Communication (RVAC) where the central authority lies on the first tier to perform the verification of nodes. RSUs remain on the second tier that enable V2I communication among nodes on the third tier. The authors in [30] propose a Situation-Aware Trust (SAT) architecture. SAT comprises three major components for enabling efficient and reliable inter-node communication. The components include (1) an attributes oriented control policy, (2) a proactive model to enable trust among nodes, and (3) an email enabled network. The authors in [31] propose a cross-layer architecture, which segments the road and distributes the service channels among the segments for load balancing. The proposed architecture also prevents broadcast floods. The work in [32] introduces a hybrid architecture, which includes a novel concept of routing module integration layer. The proposed architecture employs two-tier routing module selection mechanism for enhanced message delivery.

The authors in [33] propose a new cloud-based architecture for VANETs, which is composed of two components, namely Vehicular Cloud Computing (VCC) and Information Centric Network (ICN). VCC helps to create a vehicular cloud for information, whereas ICN enables efficient communication of nodes with the cloud. Similar cloud-based VANET architectures are proposed in [34,35]. The work in [36] proposes a VANET architecture that analyzes the information gathered from different layers to predict congestion. The authors in [37] propose another hybrid architecture, which combines the standard IEEE 802.11p with 4G LTE to enable efficient and reliable delivery of warning messages. The authors in [38] propose a Software Defined Network (SDN) based VANET architecture to enable geo-broadcasting. This architecture employs the standard OpenFlow protocol and enables application customization by network operators. However, since collection of all the intelligence on a single centralized controller is not a good approach, the authors in [39] propose a decentralized SDN-based architecture for VANETs.

From the review of the existing VANET communication architectures, it is found that the existing literature lacks a dedicated direction-aware communication architecture to minimize collisions on bi-directional highways. Moreover, since the existing architectures do not take the direction component into consideration, this adversely impacts the collision prediction process. Furthermore, the existing architectures rely upon fixed deceleration as a preventive measure. Additionally, the existing architectures ensure message authentication but fail to provide warning messages confidentiality. Moreover, the existing architectures, for not being direction-aware, fail to cater for the frequent topological changes on bi-directional highways, which remains critical during warning messages dissemination. Finally, un-prioritized delivery of warning message is yet another critical limitation of the existing VANET communication architectures. To address these issues, we propose a novel cross-layer V2V architecture, which is detailed in the following section.

3. Direction-Aware Vehicular Collision Avoidance (DVCA) Architecture

This section presents the proposed DVCA architecture using V2V communications for bi-directional highways, as depicted in Figure 2. DVCA comprises a protocol suite consisting of application, security services, network, MAC and physical layers, as shown in Figure 1. Figure 3 depicts the layer-wise attributes of the proposed DVCA architecture. The working of each layer of the proposed architecture is described in the following subsections. Table 1 lists the notations used in this paper.

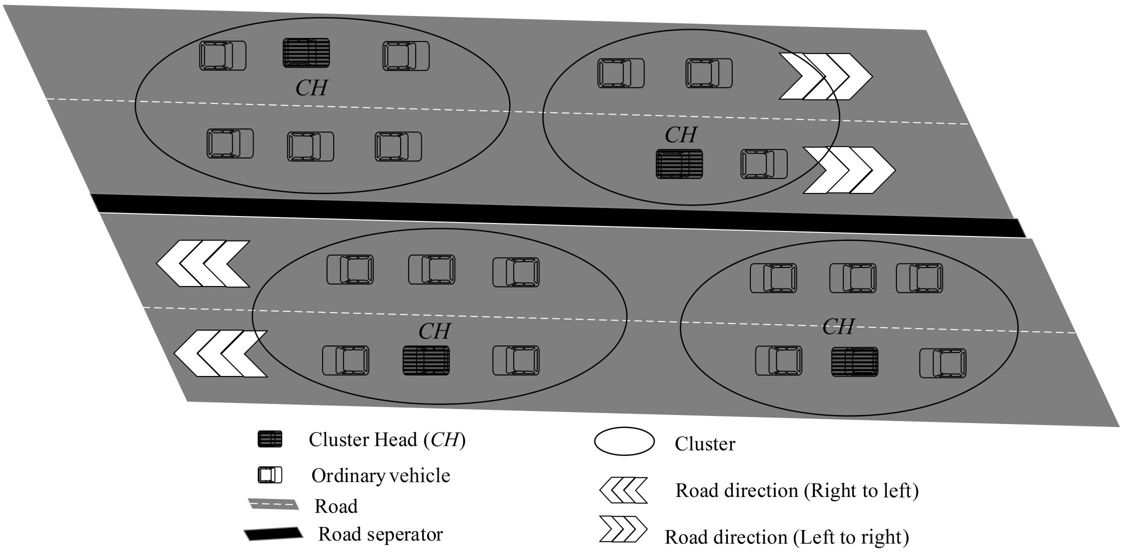


Figure 2. A bi-directional highway scenario.

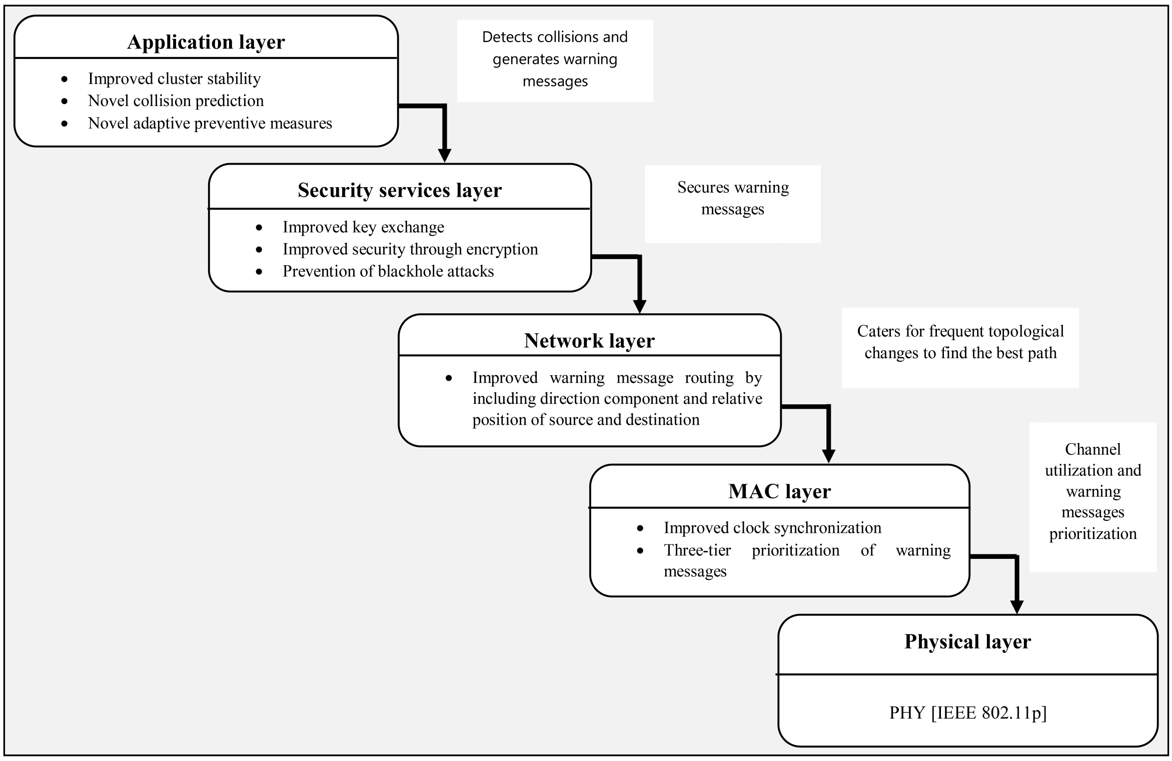

Application layer
Improved cluster stability
Novel collision prediction
Novel adaptive preventive measures
Detects collisions and generates warning messages
Security services layer
Improved key exchange
Improved security through encryption
Prevention of blackhole attacks
Secures warning messages
Network layer
Improved warning message routing by including direction component and relative position of source and destination
Caters for frequent topological changes to find the best path
MAC layer
Improved clock synchronization
Three-tier prioritization of warning messages
Channel utilization and warning messages prioritization
Physical layer
PHY [IEEE 802.11p]

Figure 3. Layer-wise attributes of the proposed DVCA architecture.

Table 1. Notations.

Notation	Description
A_c	Acceleration or deceleration attained by a node
C_s	Circular shift value
CH	A cluster head
χ	Set of nodes' speeds
D	Destination node
δ	Benign factor
Δ	Final distance among nodes
κ	Hamming distance among nodes
key	Unique symmetric key for encryption
Loc_c	Current state of a node
Loc_e	Expected state of a node
L	Severity level of warning messages
NW	Non-warning message
P_c	Probability of collision
P_k	Public key
PID	Public identity of a node
rv	Random vector
S	Source node
SID	Secret identity of a node
σ	Authentication hash
τ	Next time step
V_c	Current speed of a node
V_f	Current speed of the front node
V_r	Current speed of the rear node
V_s	Safe speed for a node
W	Warning message

3.1. DVCA Application Layer

The application layer of DVCA implements our direction-aware CCA application [15] to identify possible collisions among nodes on bi-directional highways and specify preventive measures. DVCA starts with nodes' clustering using our variant of the *k*-medoids clustering algorithm, proposed in [15], which provides improved cluster stability with minimal clustering overhead in a V2V environment. Cluster stability is achieved by employing the direction component, besides using relative distances among nodes, during the clustering process, as [15]

$$\Delta_i = \frac{|n_x^i - CH_x^i| + |n_y^i - CH_y^i|}{\kappa(n^i, CH^i)}. \tag{1}$$

Here, Δ is the final distance between a node n and the CHs, and κ represents the Hamming distance between them. The next step computes the probability of collision among nodes based on the nodes' expected states. The expected state of a node is predicted as [15]

$$Loc_e = Loc_c + (V_c\tau + \frac{1}{2}A_c\tau^2). \tag{2}$$

Here, Loc_e and Loc_c are the expected and current states of a node, respectively, V_c represents the current speed of the node, τ is the next time step, and A_c represents the acceleration or deceleration attained. By taking into account the expected states of nodes, DVCA is able to extend the time for nodes to react to hazardous events, thereby, providing effective means to reduce collisions [15]. Moreover, a warning message is generated only if the probability of collision (P_c), computed using Equation (3) [15], exceeds a predefined threshold that seeks to reduce the communication overhead.

$$P_c = \left[1 - \frac{\left\{\Big((V_f - V_r)\,\tau \,+\, \Delta\Big) - \varrho\right\}}{(\iota - \varrho)}\right]\kappa. \tag{3}$$

Here, V_f and V_r represent the speed of front and rear nodes, respectively, and ϱ and ι are the minimum and maximum scores evaluated from the fraction $\Big((V_f - V_r)\,\tau \,+\, \Delta\Big)$, respectively.

Since preventive measures are also specified at the application layer, DVCA computes safe speeds (V_s) using Equation (4) by employing our adaptive deceleration technique, called the Benign factor (δ) [15], which ranges from 0 to 1.

$$V_s = V_c\delta. \tag{4}$$

Thus, deceleration does not remain constant in all scenarios in DVCA, rather it varies in different situations. The estimated collision probability along with the safe speed constitutes a warning message, which is passed to the security services layer before dissemination to the target node.

3.2. DVCA Security Services Layer

A warning message, intended to alert a target node to slow down to avoid a possible collision, may be intercepted by a malicious node that can discard the message or modify it to cause a collision. Overcoming such critical situations demands secure transmission of warning messages, which is the responsibility of the security services layer. To this end, DVCA provides enhanced nodes' privacy preservation and messages authentication. Reliable and fast key exchange among nodes is one of the biggest issues in VANETs, which is achieved by using our variant of the Diffie–Hellman key exchange algorithm, proposed in [16], as follows.

CH^i:

$\beta_{CH^i} \longleftarrow \mathrm{P}_k \odot \mathrm{SID}_{CH^i}$

```
    $CH^i$ sends $(\beta_{CH^i} \mid\mid \tau)$ to $n^i$
$n^i$:
    $\beta_{n^i} \longleftarrow \mathrm{P}_k \odot \mathrm{SID}_{n^i}$
    $n^i$ sends $(\beta_{n^i} \mid\mid \tau)$ to $CH^i$
$CH^i$:
    $CH^i$ generates $key$
    $key_i \longleftarrow \beta_{n^i} \odot \mathrm{SID}_{CH^i}$
$n^i$:
    $n^i$ generates $key$
    $key_i \longleftarrow \beta_{CH^i} \odot \mathrm{SID}_{n^i}$
```

Here, P_k represents the public key, SID is the secret identity of a node, and *key* is the unique symmetric key exchanged through the aforementioned process.

After the keys are successfully exchanged, DVCA encrypts the warning message by using our light-weight encryption algorithm [16], which secures warning messages from intruders. The warning messages are encrypted as below.

```
Random generation of $1 \times 4$ matrix, $Y$
  **For** $j$ = 1 **To** 4
    **Switch**($Y$(j))
      **Case:** 1
        **For** $x$ = 1 **To** size($W$) - 1
          $W(x) \longleftarrow W(x) \oplus W$(x+1)
        **End For**
          $W \longleftarrow W \oplus key_i$
      **Case:** 2
        $W \longleftarrow$ Circular-shift($W$, $C_s$)
      **Case:** 3
        Generate the random vector, $rv$
        $W \longleftarrow W \oplus rv$
      **Case:** 4
        Byte-wise substitution operation
    **End Switch**
  **End For**
```

DVCA then generates the authentication hash as follows, which is appended to the warning message (W) obtained from the aforementioned encryption process,

$$\sigma_s = PID_s \odot PID_d \odot W \odot \tau \odot key_i. \tag{5}$$

Here, σ_s represents the authentication hash generated at a source node and PID is the public identity of a node, which is used for communication with other nodes. A predefined threshold, which indicates the time to retransmit warning messages if no acknowledgments are received by the source nodes, is maintained to avoid blackhole attacks. The retransmission occurs through an alternative path and the corresponding CH notifies the previous path as suspicious of malicious activities. On successful encryption of the warning message, the cipher text is handed over to the network layer so that it can be routed to the destination node.

3.3. DVCA Network Layer

The responsibility of the network layer is to enable timely and reliable transmission of warning messages [40]. VANETs experience frequent topology changes due to high speed nodes on bi-directional highways. This results in frequent path reconstruction processes, as nodes frequently enter and exit the communication range of each other. To encounter such changes, DVCA introduces two additional parameters besides the distance parameter. These parameters include the direction component and the relative position of the source and destination nodes, which help to find the most suitable path among the available set of paths [17]. When a rear source node (S) intends to transmit a warning message to destination (D) having $\kappa(S, D) = 1$, Δ between D and the next hop (H) is computed as [17]

$$\Delta(D, H) = \frac{|H_x - D_x| + |H_y - D_y|}{\kappa(S, H)}. \tag{6}$$

In a case, where D remains rear to S, Δ is computed as [17]

$$\Delta(D, H) = (|H_x - D_x| + |H_y - D_y|)\, \kappa(S, H). \tag{7}$$

Similarly, when S and D exhibit opposite directions, Equation (6) is used to compute Δ when these nodes are moving towards each other, whereas Equation (7) is used when S and D are moving away from one another. Such a direction-aware routing process to find the best enhances network throughput, and reduces packets drop ratio and end-to-end delays that results in timely delivery of warning messages [17]. The network layer then hands over the warning message to the MAC layer.

3.4. DVCA MAC Layer

At the MAC layer, DVCA performs inter-cluster as well as intra-cluster clock synchronizations. Thus, local clocks of the member nodes of all clusters on a bi-directional highway get synchronized to a common clock in order to improve channel utilization. Moreover, since warning messages are time-critical, our three-tier priority assignment algorithm, proposed in [18], is used to transmit critical warning messages at higher priority. The first tier takes the direction component into account and selects a relay node bearing direction towards the destination node using Equations (6) and (7) in a similar manner to the network layer. The second tier bifurcates (W)s and non-warning messages (NW)s, and assigns higher priority to (W)s. The third tier differentiates among warning messages of different severity levels, which helps to disseminate highly critical warning messages on top priority. Here, DVCA sets the severity level based on the collision probability computed at the application layer, as shown in Table 2. This tier prioritizes the warning messages further as below.

```
Switch($L$)
    Case: $L_0$
        Wait for a free time slot
    Case: $L_1$
        Request to release a time slot
    Case: $L_2$
        Release a reserved time slot by a non-warning or low priority warning message.
End Switch
```

Table 2. Warning messages' severity levels.

L	Range of P_c
NW	$P_c = 0.00$
L_0	$(P_c > 0.00)$ and $(P_c <= 0.33)$
L_1	$(P_c > 0.33)$ and $(P_c <= 0.66)$
L_2	$(P_c > 0.66)$ and $(P_c <= 1.00)$

The aforementioned prioritized dissemination process enhances channel utilization and throughput, and results in reduced warning message drop rate and end-to-end delays [18].

DVCA uses the standard IEEE 802.11p at the physical layer. Once a warning message is received by a destination node, the destination node decrypts and authenticates the message and adopts the communicated preventive measures, i.e., the safe speed, to avoid a possible collision. Figure 4 presents the procedural flowchart of the proposed DVCA architecture.

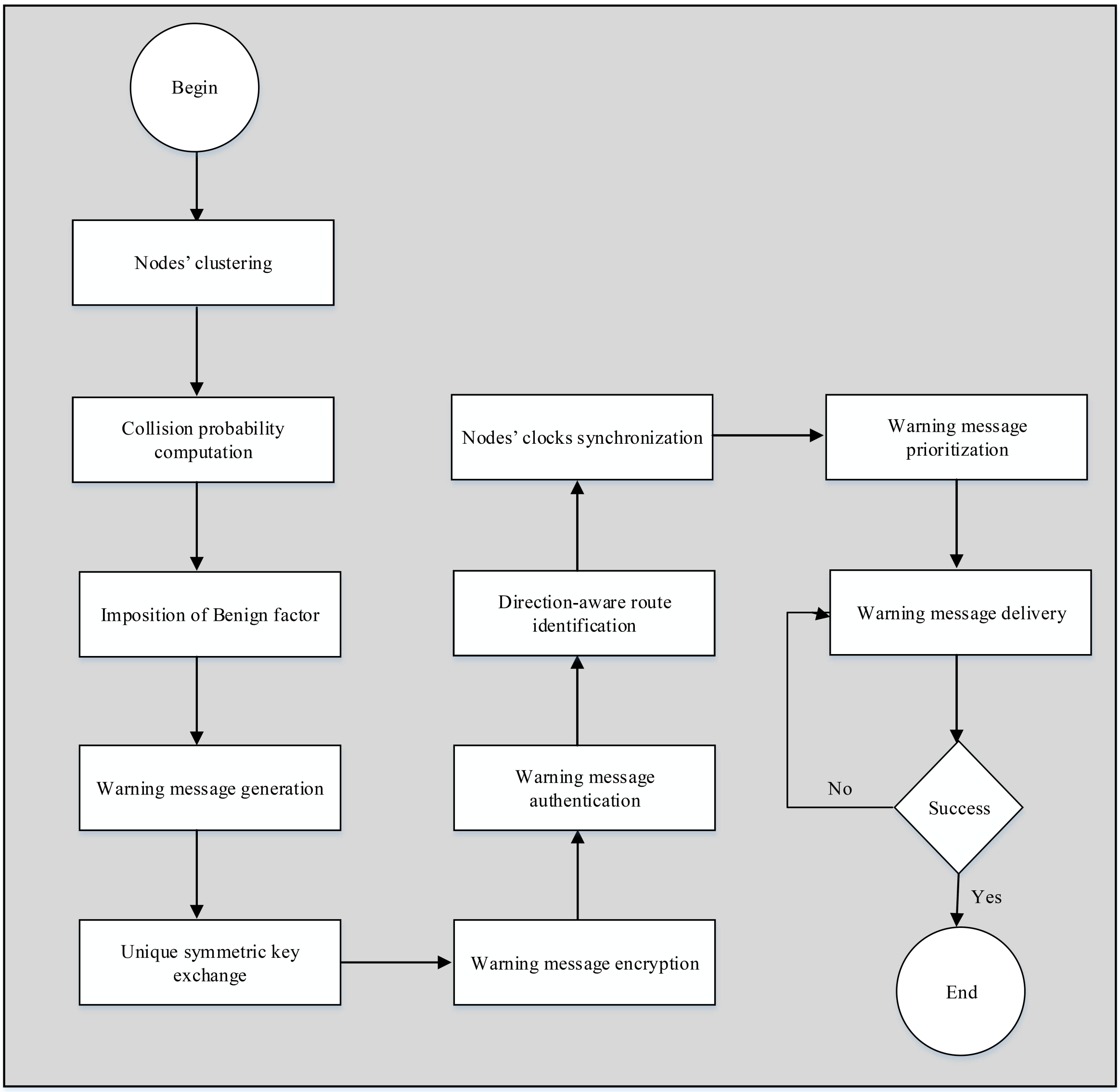

Begin
Nodes' clustering
Collision probability computation
Imposition of Benign factor
Warning message generation
Unique symmetric key exchange
Warning message encryption
Warning message authentication
Direction-aware route identification
Nodes' clocks synchronization
Warning message prioritization
Warning message delivery
Success
No
Yes
End

Figure 4. Procedural flowchart of the proposed DVCA architecture.

4. Performance Evaluation

This section evaluates the proposed DVCA architecture compared with two different variants of the WAVE architecture, referred to as WAVE-A and WAVE-B. WAVE-A employs Cluster-based Risk-Aware Cooperative Collision Avoidance (C-RACCA) [6], Enhanced-CPPA (E-CPPA) [41], Path Aware-Greedy Perimeter Stateless Routing (PA-GPSR) [42], and Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) [43] at application, security services, network, and MAC layers, respectively. Similarly, WAVE-B employs Collision Computation Model (CCM) [44], Registration List-based CPPA (RL-CPPA) [45], Improved Directional- Location Added Routing (ID-LAR) [46], and Distributed Multi-Channel MAC (DMCMAC) [47] at application, security services, network, and MAC layers, respectively. Likewise, DVCA has P-DACCA [15], LWE-CPPA [16], DABFS [17], and PDMAC [18] on its application, security services, network, and MAC layers, respectively.

The physical layer standard for the three competing collision avoidance architectures is PHY IEEE 802.11p. Figure 5 depicts a comparison of the protocol suites of the three competing collision avoidance architectures. The simulation area is taken as 2500 m × 1200 m. The number of nodes ranges from 1–100, where each node moves with randomly assigned speed belonging to χ in a bi-directional highway scenario, as depicted in Figure 2. Simulation results are derived using ns-2.35. For security analysis, the Automated Validation of Internet Security Protocols and Applications (AVISPA) [16] and Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL) [48] are used. The results are averaged over 20 replicated runs using different random seed values. Table 3 presents the simulation parameters. Simulation results of the proposed DVCA architecture are validated through analytical results obtained on MATLAB (R2018a).

Since the objective of this paper is to evaluate the cumulative effect of our complete protocol suite (shown in Figure 1) in mitigating collisions, in this section we consider security validation, computational overhead, communication overhead, reliable and in-time delivery of warning messages, inter-cluster collision avoidance and the effects of relative distance and speed on collisions as the performance evaluation metrics. Detailed performance metrics pertaining to each layer have been considered in our previous works [15–18], where each of the proposed protocol has been shown to outperform eminent existing protocols of the corresponding layer.

Table 3. Parameters for simulations.

Parameter	Configuration
Area of simulation	2500 m × 1200 m
Node length	4 m
Propagation model	TwoRayGround
Traffic type	Bi-directional highway
δ	0.00–1.00
Node's communication range	150 m
Collision probability threshold	0.50
Simulation time	180 s
χ	0–42 m/s
Synchronization interval	100 ms
Number of nodes	1–100

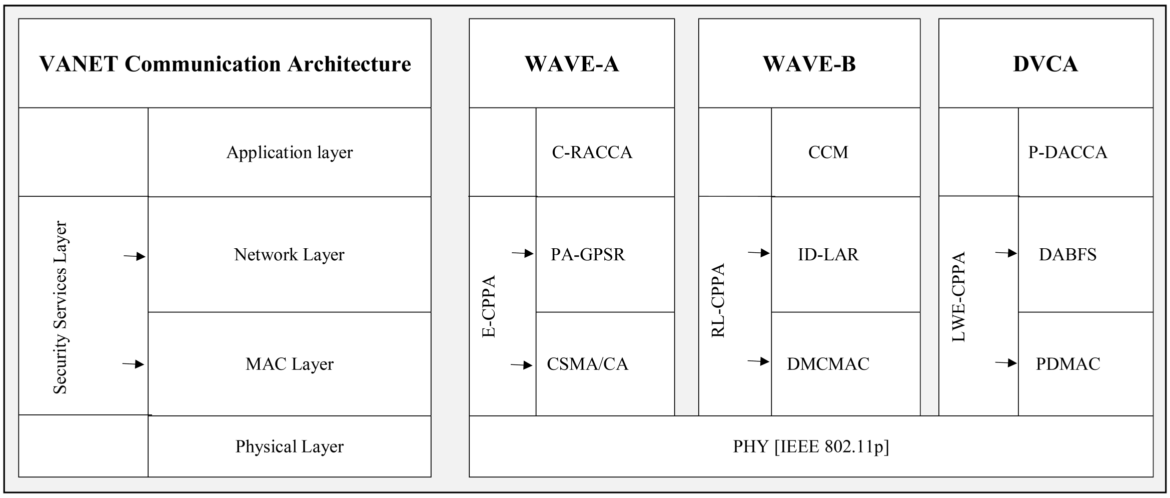
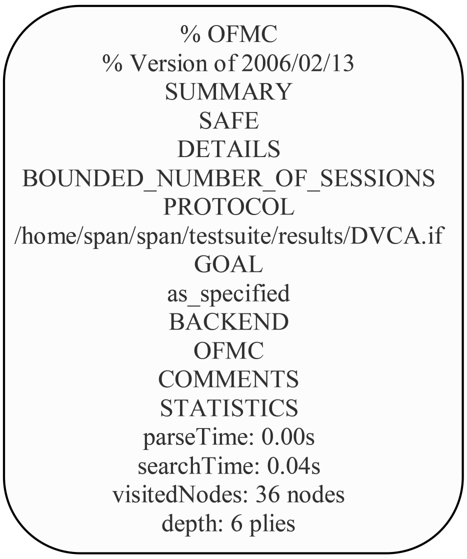


Figure 5. Comparison of VANET collision avoidance protocol suites.

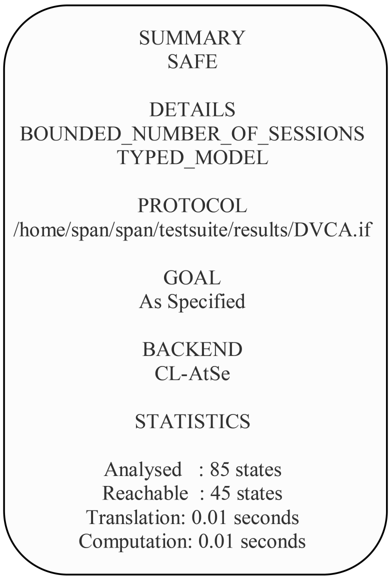
4.1. Security Validation

To validate the security features of the proposed DVCA architecture, we used AVISPA and conduct several experiments using Security Protocol Animator (SPAN) [16]. The experiments were conducted using a Linux-based machine having Core i5-6300 processor with 8 gigabytes of memory. Two AVISPA models, namely, On-the-Fly-Model-Checker (OFMC) and the Constraint-Logic-based Attack Searcher (CL-AtSe) were used for security validation. The OFMC model verified the protocol security, syntax, semantics, and correctness, whereas the CL-AtSe model validated the security of a protocol against a number of attacks. Results depicted in Figures 6 and 7 demonstrated that DVCA was *safe* with respect to the aforementioned AVISPA models.



```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span/span/testsuite/results/DVCA.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.04s
visitedNodes: 36 nodes
depth: 6 plies
```

Figure 6. Security validation of DVCA through On-the-Fly-Model-Checker (OFMC) model (AVISPA).



```
SUMMARY
SAFE

DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL

PROTOCOL
/home/span/span/testsuite/results/DVCA.if

GOAL
As Specified

BACKEND
CL-AtSe

STATISTICS

Analysed   : 85 states
Reachable  : 45 states
Translation: 0.01 seconds
Computation: 0.01 seconds
```

Figure 7. Security validation of DVCA through Constraint-Logic-based Attack Searcher (CL-AtSe) model (AVISPA).

4.2. Computational Overhead

Computational overhead is one of the factors affecting the in-time delivery of warning messages [16], thus, reducing this overhead enables fast delivery of warning messages. This extends the reaction time to apply the preventive measures that helps in minimizing the collisions among nodes, as demonstrated in Sections 4.5–4.7. Thus, besides providing security, the security services layer should also minimize the computational overhead in securing time-sensitive warning messages.

To this end, DVCA reduced the computation time reasonably by effectively using logical operations and excluding computationally expensive operations, such as *mod*. Results depicted in Figure 8 show reasonably minimized computation time for DVCA, compared to WAVE-A and WAVE-B, in securing the warning messages.

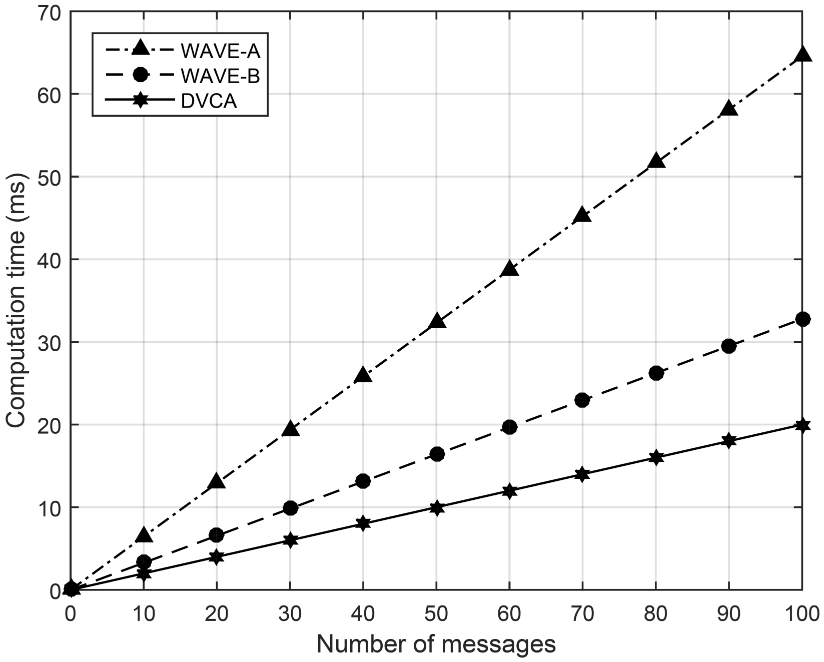


Figure 8. Computational time for encryption and authentication of warning messages.

4.3. Communication Overhead

DVCA minimizes the communication overhead by reducing the size of the ciphertext generated as a result of encryption and authentication process performed on warning message. The results depicted in Figure 9 show minimized communication overhead for DVCA in comparison with WAVE-A and WAVE-B. Moreover, since WAVE-A and WAVE-B were not direction-aware, unnecessary warning messages were generated for nodes travelling on the opposite side of the highway. Conversely, DVCA introduced a novel direction-aware probability computation process that restricted warning messages generation for nodes on the same side of the road only. The warning messages generation was further restricted, in DVCA, with a pre-defined threshold in terms of collision probability. Hence, a warning message was only generated when this threshold was exceeded. Results presented in Figure 10 validated this claim, where DVCA outperformed WAVE-A and WAVE-B by avoiding unnecessary warning messages generation for the nodes on the opposite side of the road. Communication overhead is yet another factor that affects the in-time delivery of time-sensitive warning messages [16]. Thus, reducing this overhead further minimized the end-to-end delays experienced during warning messages transmission. This resulted in providing extended reaction time to apply the preventive measures, which minimized the number of collisions among nodes, as demonstrated in Sections 4.5–4.7.

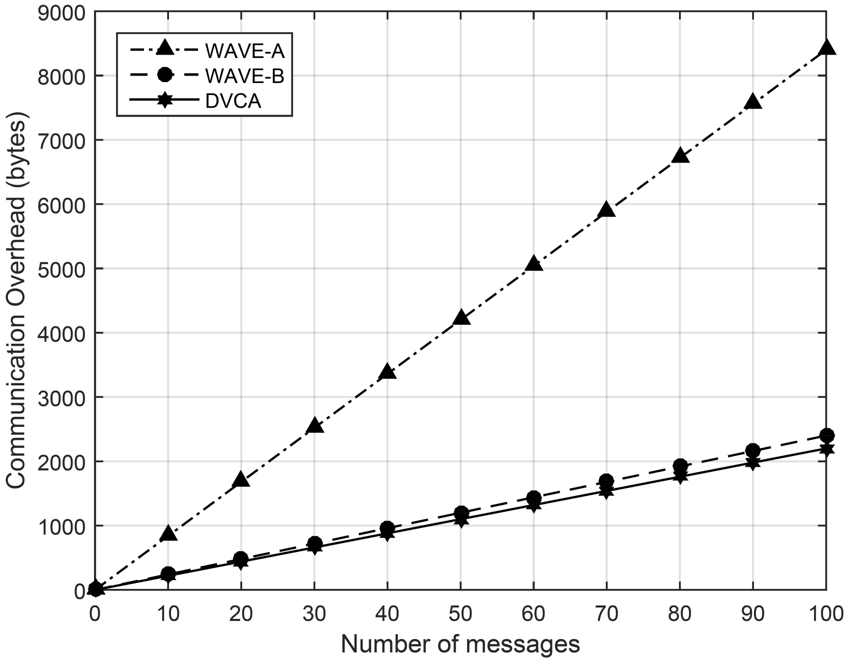


Figure 9. Impact of warning message size on communication overhead.

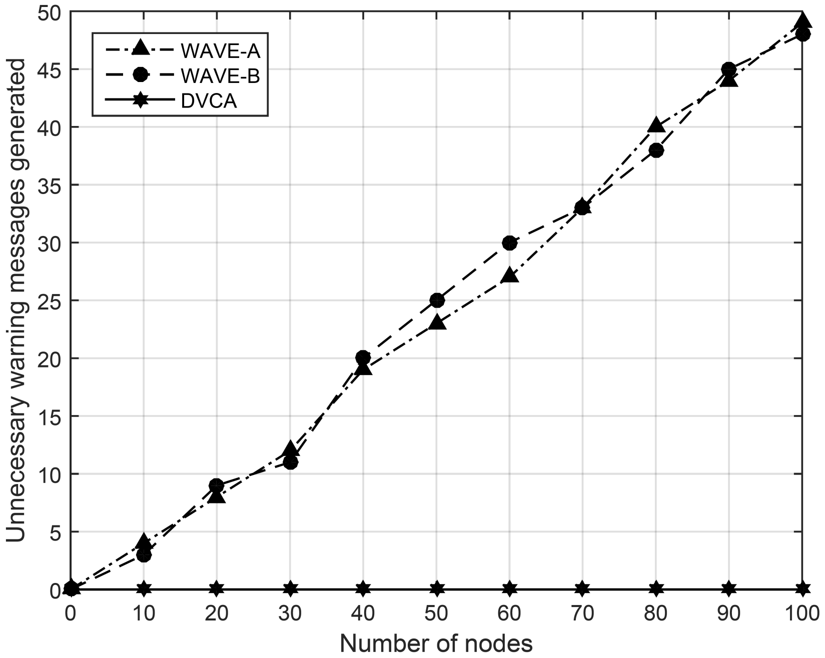


Figure 10. Unnecessary warning messages generation.

4.4. Reliable and In-Time Delivery of Warning Messages

This section evaluates the performance of the competing architectures in terms of reliable and in-time delivery of warning messages. Reliability refers to ensuring successful warning messages delivery. Reliable transmission of warning messages remains critical for collision avoidance, which is achieved by reducing the message loss ratio. DVCA provides direction-aware routing of warning messages, which reduces the message loss ratio [17]. Furthermore, DVCA employs its novel three-tier prioritization technique at MAC layer to differentiate among warning messages of different severity levels. This enables the transmission of warning messages having greater collision probability at higher priority to further reduce the warning messages loss ratio [18]. The results shown in Figure 11 validated the aforementioned claim and demonstrated the efficacy of DVCA, in terms of reduced message loss ratio, in comparison with WAVE-A and WAVE-B. Moreover, reducing the warning messages dissemination time also helped in better collision avoidance, as it provided increased reaction time for the application of preventive measures. Results presented in Figure 12 demonstrated superior performance of DVCA, in terms of reduced average warning dissemination time, in comparison with WAVE-A and WAVE-B. There were three major reasons for the better performance of DVCA: (1) reduced computational and communication overheads at the security service layer, (2) the direction-aware routing at network layer that catered for the topological changes efficiently and finds the shortest path, and (3) the three-tier prioritization process at the MAC layer.

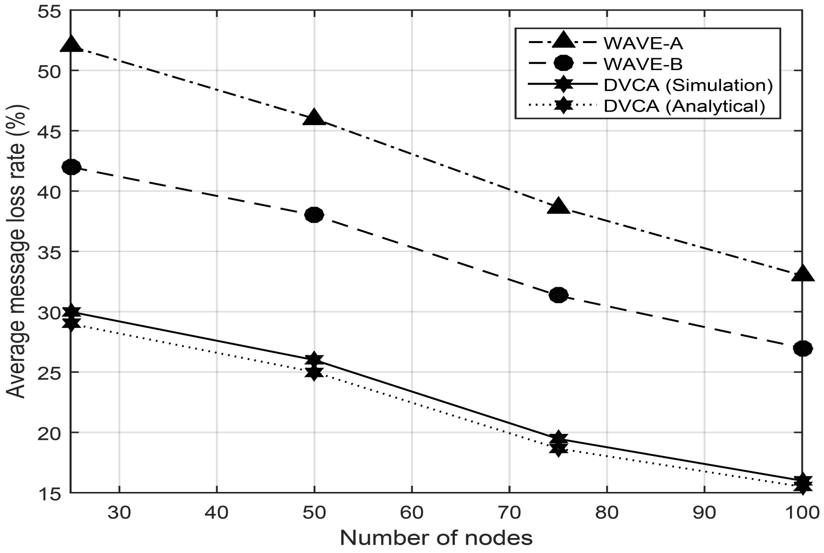


Figure 11. Average warning messages loss ratio.

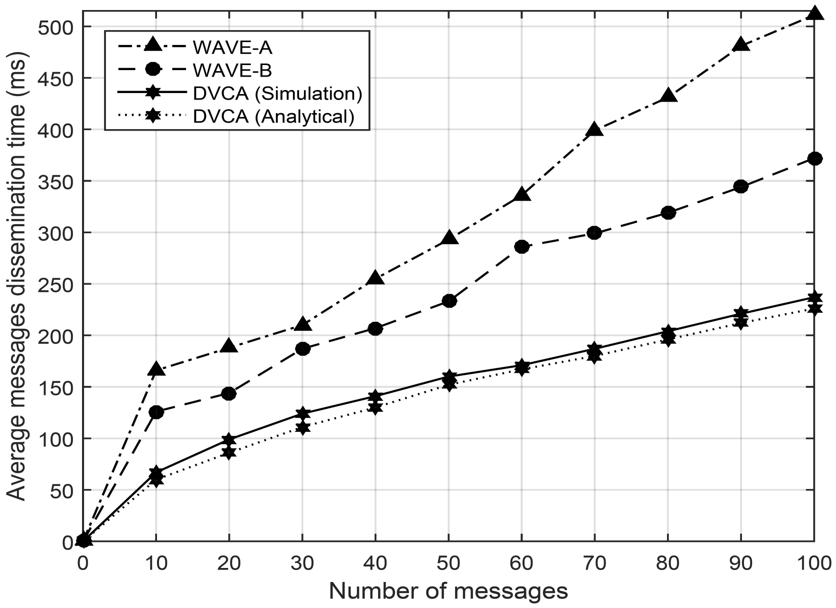


Figure 12. Average warning messages dissemination time.

4.5. Inter-Cluster Collisions

In order to evaluate the performance of the three competing architectures in terms of reducing inter-cluster node collisions, we considered a scenario that took clusters in the range 5–20. The maximum number of member nodes in each cluster was 5. An initial distance of 5 m was taken among clusters, which varied as the nodes in each cluster moved with respect to their randomly assigned speeds from the set χ. Figure 13 demonstrates the results that compared DVCA, WAVE-A, and WAVE-B in terms of inter-cluster node collisions. Here, DVCA showed improved efficiency by 37.25% and 35.0% in comparison with WAVE-A and WAVE-B, respectively, due to its efficient collision prediction process and adaptive preventive measures. Moreover, the direction-aware, timely, and reliable warning messages dissemination at network and MAC layers in DVCA also played a key role in reducing collisions among nodes that lay near the edges of their corresponding clusters.

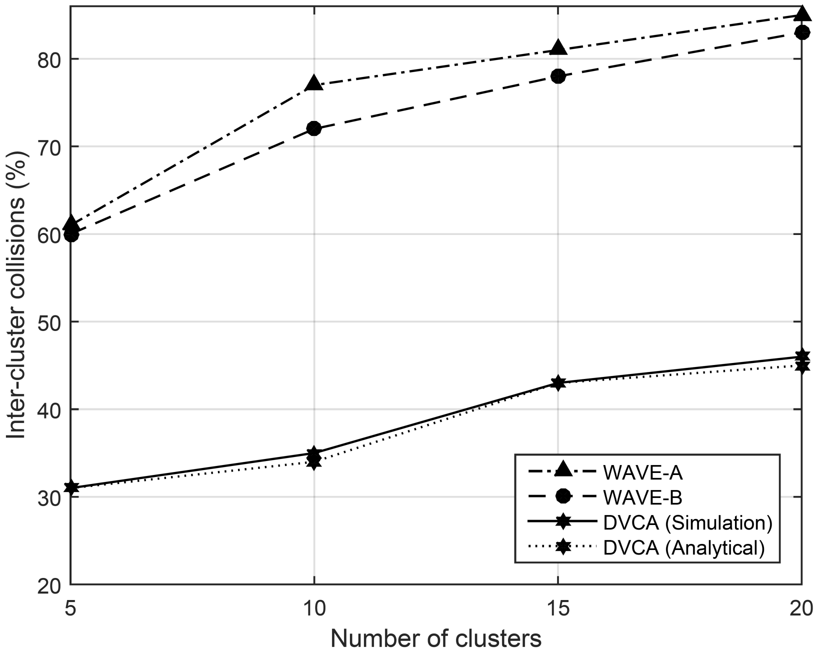


Figure 13. Inter-cluster collision avoidance.

4.6. Effect of Relative Distance on Collisions

This section compares the performance of the competing collision avoidance architectures with respect to the effect of relative distance on nodes' collisions. A scenario with 100 nodes, deployed initially with a relative distance that ranges between 5–25 m, was considered. Safe distance among nodes was taken as the distance covered by nodes in 2 s, which remained a function of the nodes' speeds [49]. Since the number of collisions decreased with increase in the relative distance among nodes, this behavior was exhibited by all competing architectures in the results depicted in Figure 14.

WAVE-A and WAVE-B lacked efficient collision identification on bi-directional highways, as these architectures did not consider the direction component. Conversely, DVCA provided a direction-aware collision probability computation technique that resolved the aforementioned issue. Additionally, WAVE-A and WAVE-B relied on fixed deceleration as preventive measures, due to which these architectures experienced performance degradation in scenarios where a rear node exhibited higher speed in comparison with the front node. To this end, DVCA imposed an adaptive preventive measure through our Benign factor [15], which enables better collision avoidance. Moreover, in addition to efficient collision identification and preventive measures, timely and reliable delivery of warning messages also remains critical. In this regard, DVCA took into account the direction component in finding the most appropriate path to a destination node, which was found lacking in WAVE-A and WAVE-B architectures.

Furthermore, wireless channel utilization is also important to ensure efficient warning messages delivery. Since WAVE-A and WAVE-B assigned the same priority to both warning and non-warning messages, the warning messages either got dropped or experienced extensive end-to-end delays when the ratio of non-warning messages increased. To this end, DVCA employed a three-tier priority assignment technique, which enabled enhanced warning messages delivery in comparison with WAVE-A and WAVE-B. Reliable and timely transmission of warning messages provided a favourable environment to timely apply the preventive measures, thereby, reducing the number of collisions. The results shown in Figure 14 validated the efficacy of DVCA with average improved performance of 44.6% and 26.4%, as compared with WAVE-A and WAVE-B, respectively.

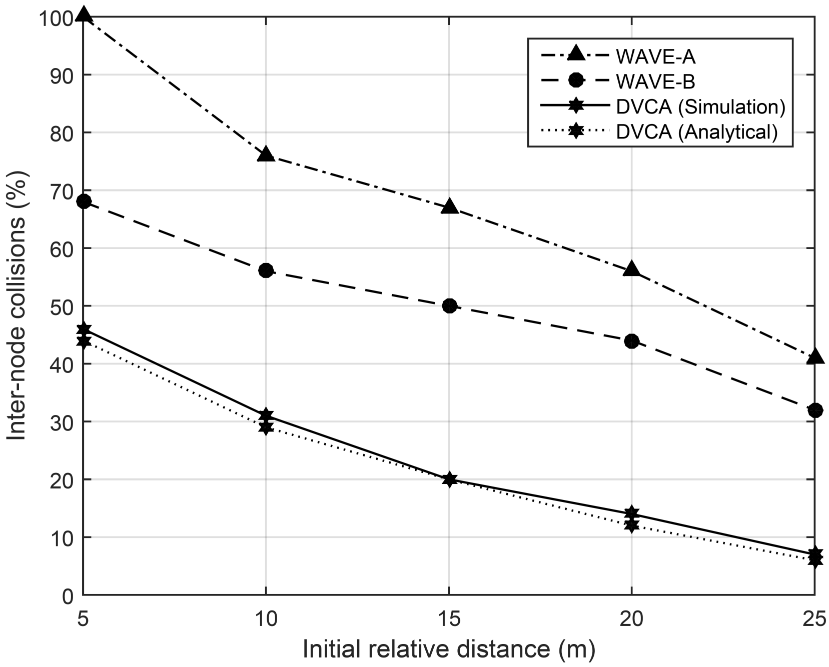


Figure 14. The effect of relative distance on collisions.

4.7. Effect of Relative Speed on Collisions

This section analyzes the impact of relative speed upon collisions. A total number of 100 nodes were taken, where each node was assigned a random speed in the range 0–42 m/s. A 7 m/s speed interval was taken to observe and record collisions. Initially, the distance among nodes was taken between 5–30 m. The distance varied when the nodes continued to move with random speeds assigned within χ.

The speed of nodes was a major reason for collisions. Since both WAVE-A and WAVE-B relied upon fixed deceleration to prevent collisions, these architectures experienced performance degradation in situations where rear nodes exhibited higher speeds in comparison to the front nodes. In such scenarios, a fixed deceleration became incapable of preventing the possible collisions. Conversely, DVCA performed adaptive deceleration for collision avoidance. The safe speed was computed in accordance with the speed of the front node and the deceleration rate remained proportional to the speed of the rear node. Moreover, network and MAC layers of DVCA remained direction-aware during the transmission of warning messages, which provided reliable and timely delivery of warning messages. The results presented in Figure 15 demonstrated that DVCA yielded much fewer collisions with average improved performance of 19.0% and 12.0% compared with WAVE-A and WAVE-B, respectively.

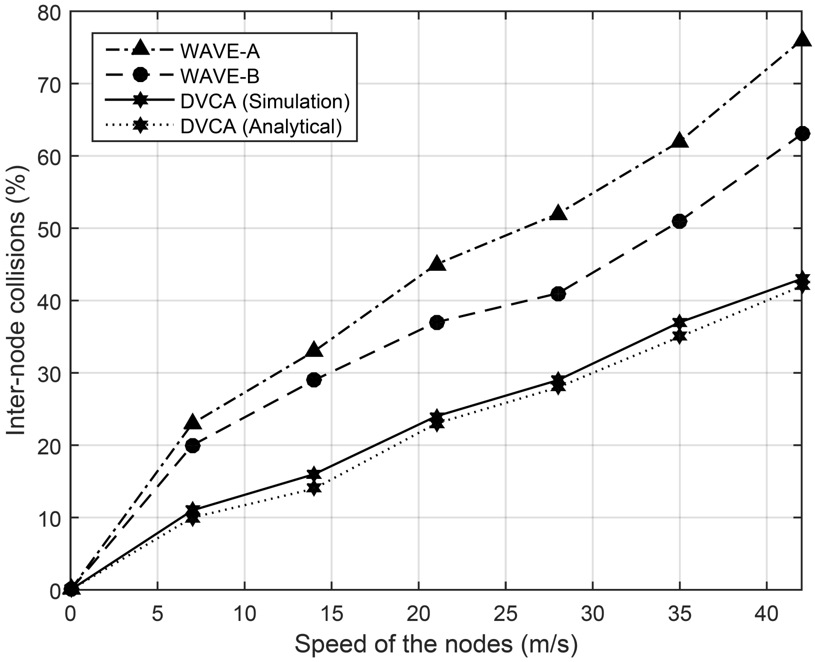


Figure 15. The effect of relative speed on collisions.

4.8. Critical Discussion

Since highway collisions are one of the major causes of casualties around the world today, this makes collision avoidance an enticing area of research. Modern transportation systems employ VANETs for improving traffic flow, travel time estimation, route identification, and collision avoidance. The existing VANET communication standards, such as WAVE, comprise a layered architecture with a protocol suite. These architectures can be utilized for developing various VANET applications, such as infotainment, route identification, and collision avoidance. However, for efficient collision avoidance, a number of challenges must be addressed across all layers of the architecture. Our previous works [15–18] have addressed layer-wise challenges related to collision avoidance on bi-directional highways using V2V communications. Each proposed protocol has been demonstrated to outperform eminent existing protocols of the corresponding layer. However, for performance evaluation in [15–18], only the performance metrics of the corresponding layer were taken into account. For generating simulation results of a particular protocol, standard protocols were used at all other layers.

This paper has presented a novel V2V architecture, called Direction-Aware Vehicular Collision Avoidance (DVCA), which consolidates our previous works [15–18] into a complete protocol suite. The proposed collision avoidance architecture includes P-DACCA [15], LWE-CPPA [16], DABFS [17], and PDMAC [18] at its application, security services, network, and MAC layers, respectively, as shown in Figure 1. The paper then evaluates the cumulative effect of the protocol suite. We have shown in this paper that collision avoidance can not only be enhanced by efficient clustering, effective probability computation, and adaptive preventive measures at the application layer, but it can also be improved by considering the direction component on network and MAC layers. Simulation and analytical results presented in this section validate the efficacy of DVCA, in terms of reduced collisions among nodes in comparison with eminent VANET architectures. Section 4.1 has validated the security features of DVCA using the OFMC and CL-AtSe models of AVISPA to demonstrate that DVCA is $safe$. Sections 4.2 and 4.3 have evaluated the computational and communication overheads, respectively. DVCA has been shown to reasonably reduce both of the overheads in comparison with other eminent architectures.

The reduced overheads along with direction-aware prioritized warning messages dissemination result in reduced average warning message dissemination time for DVCA in comparison with the other architectures. The results demonstrated in Section 4.4 have indicated improved performance of DVCA, in terms of reasonably reduced message loss ratio and warning messages dissemination time to enable reliable and in-time warning messages delivery. Section 4.5 has compared performance with respect to inter-cluster collision avoidance, where DVCA has demonstrates improved efficiency by 37.25% and 35.0% in comparison with WAVE-A and WAVE-B, respectively. Section 4.6 has evaluated the performance of DVCA with respect to the effect of relative distance on collisions, in comparison with eminent VANET architectures. It is shown that DVCA reduces collisions by 44.6% and 26.4% in comparison with WAVE-A and WAVE-B, respectively. Moreover, Section 4.7 has evaluated the relationship between the nodes' collisions and the relative speeds. Once again, DVCA exhibited superior performance in terms of reduced collisions by 19.0% and 12.0%, compared with WAVE-A and WAVE-B, respectively. Thus, DVCA can be deployed as an effective tool to reduce collisions on bi-directional highways.

The limitation of DVCA, however, is that it is not designed for urban environments comprising intersections. This limitation will be addressed in our future work. Another research direction is to present a more suitable PHY protocol for DVCA.

5. Conclusions

Due to the ever-increasing number of road accidents on highways, collision avoidance has attracted a much broader attention of the ITS research community. VANETs have emerged as a promising solution to prevent collisions by enabling CCA applications. Collision prediction and specification of preventive measures remain the prime concern of the CCA applications, while secure, reliable, and timely delivery of warning messages also remain critical. This makes collision avoidance a cross-layer problem. This paper has presented a novel direction-aware V2V communication architecture for collision avoidance, named DVCA, which comprises of a stack of our previously proposed protocols for mitigating collisions on bi-directional highways. The proposed architecture provides improved collision probability computation and adaptive preventive measures, which are encapsulated in a warning message to alert nodes about possible collisions. DVCA also enables secure, in-time and reliable dissemination of warning messages and extends the time for nodes to react and prevent collisions. As compared with eminent VANET communication architectures, simulation and analytical results have demonstrated reasonable performance improvement of DVCA for it to be deployed as an effective tool to reduce highway collisions. Our future work will extend DVCA to cater for intersections in the urban environments.

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

Funding: This work is partially supported by The China's National Key R&D Program (No. 2018YFB0803600), Natural Science Foundation of China (No. 61801008), Beijing Natural Science Foundation National (No. L172049), Scientific Research Common Program of Beijing Municipal Commission of Education (No. KM201910005025) and Defence Industrial Technology Development Program (No. JCKY2016204A102).

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

References

1. Halim, Z.; Kalsoom, R.; Bashir, S.; Abbas, G. Artificial intelligence techniques for driving safety and vehicle crash prediction. *Artif. Intell. Rev.* **2016**, *46*, 351–387.
2. Evelyn, M. *Global Status Report on Road Safety*; World Health Organization (WHO): Geneva, Switzerland, 2019.

3. Hîrţan, L.A.; Dobre, C.; González-Vélez, H. Blockchain-based reputation for intelligent transportation systems. *Sensors* **2020**, *20*, 791.
4. Ganin, A.A.; Mersky, A.C.; Jin, A.S.; Kitsak, M.; Keisler, J.M.; Linkov, I. Resilience in Intelligent Transportation Systems (ITS). *Transp. Res. Part C Emerg. Technol.* **2019**, *100*, 318–329.
5. Abd El-Gawad, M.A.; ElSawy, H.; Sakr, A.H.; Kim, H. Network-Wide Throughput Optimization for Highway Vehicle-To-Vehicle Communications. *Electronics* **2019**, *8*, 830.
6. Taleb, T.; Benslimane, A.; Letaief, K.B. Toward an effective risk-conscious and collaborative vehicular collision avoidance system. *IEEE Trans. Veh. Technol.* **2010**, *59*, 1474–1486.
7. Saraereh, O.A.; Ali, A.; Khan, I.; Rabie, K. Interference Analysis for Vehicle-to-Vehicle Communications at 28 GHz. *Electronics* **2020**, *9*, 262.
8. Harding, J.; Powell, G.; Yoon, R.; Fikentscher, J.; Doyle, C.; Sade, D.; Lukuc, M.; Simons, J.; Wang, J. *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*; Technical Report; United States National Highway Traffic Safety Administration: Washington, DC, USA, 2014.
9. Joerer, S.; Segata, M.; Bloessl, B.; Cigno, R.L.; Sommer, C.; Dressler, F. To crash or not to crash: Estimating its likelihood and potentials of beacon-based IVC systems. In Proceedings of the IEEE Vehicular Networking Conference (VNC 2012), Seoul, Korea, 14–16 November 2012; pp. 25–32.
10. Nyerges, Á.; Tihanyi, V. Trajectory Planning for Automated Vehicles– A Basic Approach. In Proceedings of the Vehicle and Automotive Engineering (VAE 2018), Miskolc, Hungary, 23–25 May 2018; pp. 403–412.
11. Cooper, C.; Franklin, D.; Ros, M.; Safaei, F.; Abolhasan, M. A comparative survey of VANET clustering techniques. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 657–681.
12. Haider, S.; Abbas, G.; Abbas, Z.H. VLCS: A Novel Clock Synchronization Technique for TDMA-based MAC Protocols in VANETs. In Proceedings of the 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST 2019), Karachi, Pakistan, 10–11 December 2019; pp. 1–6.
13. Mohammad, S.A.; Rasheed, A.; Qayyum, A. VANET architectures and protocol stacks: A survey. In Proceedings of the International Workshop on Communication Technologies for Vehicles, Berlin, Germany, 23–24 March 2011; pp. 95–105.
14. Group, I.W. *IEEE Guide for Wireless Access in Vehicular Environments (WAVE)-Architecture*; 1609.0-2013; IEEE: Piscataway, NJ, USA, 2014.
15. Haider, S.; Abbas, G.; Abbas, Z.H.; Boudjit, S.; Halim, Z. P-DACCA: A Probabilistic Direction-Aware Cooperative Collision Avoidance Scheme for VANETs. *Future Gener. Comput. Syst.* **2020**, *103*, 1–17.
16. Haider, S.; Abbas, G.; Abbas, Z.H.; Muhammad, F. LWE-CPPA: A scheme for secure delivery of warning messages in VANETs. *Int. J. Ad Hoc Ubiquitous Comput.* **2019**, *34*, 17–185.
17. Haider, S.; Abbas, G.; Abbas, Z.H.; Baker, T. DABFS: A robust routing protocol for warning messages dissemination in VANETs. *Comput. Commun.* **2019**, *147*, 21–34.
18. Abbas, G.; Abbas, Z.H.; Haider, S.; Baker, T.; Boudjit, S.; Muhammad, F. PDMAC: A Priority-Based Enhanced TDMA Protocol for Warning Message Dissemination in VANETs. *Sensors* **2020**, *20*, 45.
19. Khaliq, K.A.; Chughtai, O.; Shahwani, A.; Qayyum, A.; Pannek, J. Road accidents detection, data collection and data analysis using V2X communication and edge/cloud computing. *Electronics* **2019**, *8*, 896.
20. Farooq, S.M.; Hussain, S.; Kiran, S.; Ustun, T.S. Certificate based security mechanisms in vehicular ad-hoc networks based on IEC 61850 and IEEE WAVE standards. *Electronics* **2019**, *8*, 96.
21. Khan, U.A.; Lee, S.S. Multi-Layer Problems and Solutions in VANETs: A Review. *Electronics* **2019**, *8*, 204.
22. Hussain, S.S.; Ustun, T.S.; Nsonga, P.; Ali, I. IEEE 1609 WAVE and IEC 61850 standard communication based integrated EV charging management in smart grids. *IEEE Trans. Veh. Technol.* **2018**, *67*, 7690–7697.
23. Gasmi, R.; Aliouat, M. Vehicular Ad Hoc NETworks versus Internet of Vehicles-A Comparative View. In Proceedings of the 2019 International Conference on Networking and Advanced Systems (ICNAS), Annaba, Algeria, 26–27 June 2019; pp. 1–6.
24. Molina-Masegosa, R.; Sepulcre, M.; Gozalvez, J.; Berens, F.; Martinez, V. Empirical Models for the Realistic Generation of Cooperative Awareness Messages in Vehicular Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5713–5717.
25. Sherazi, H.H.R.; Khan, Z.A.; Iqbal, R.; Rizwan, S.; Imran, M.A.; Awan, K. A heterogeneous IoV architecture for data forwarding in vehicle to infrastructure communication. *Mob. Inf. Syst.* **2019**, *2019*, 3101276.

26. Mistareehi, H.; Islam, T.; Lim, K.; Manivannan, D. A Secure and Distributed Architecture for Vehicular Cloud. In *International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 127–140.
27. Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. *Sensors* **2019**, *19*, 4954.
28. Luo, J.; Gu, X.; Zhao, T.; Yan, W. MI-VANET: A new mobile infrastructure based VANET architecture for urban environment. In Proceedings of the 2010 IEEE 72nd Vehicular Technology Conference-Fall, Ottawa, ON, Canada, 6–9 September 2010; pp. 1–5.
29. Tolba, A.; Altameem, A. A three-tier architecture for securing IoV communications using vehicular dependencies. *IEEE Access* **2019**, *7*, 61331–61341.
30. Huang, D.; Hong, X.; Gerla, M. Situation-aware trust architecture for vehicular networks. *IEEE Commun. Mag.* **2010**, *48*, 128–135.
31. Trivedi, H.; Veeraraghavan, P.; Loke, S.; Desai, A.; Singh, J. SmartVANET: The case for a cross-layer vehicular network architecture. In Proceedings of the 2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications, Singapore, 22–25 March 2011; pp. 362–368.
32. Jang, H.C.; Yang, C.K. A hybrid architecture of routing protocols for vanet with cross-layer design. In Proceedings of the 2012 International Symposium on Computer, Consumer and Control, Taichung, Taiwan, 4–6 June 2012; pp. 68–71.
33. Lee, E.; Lee, E.K.; Gerla, M.; Oh, S.Y. Vehicular cloud networking: Architecture and design principles. *IEEE Commun. Mag.* **2014**, *52*, 148–155.
34. Mallissery, S.; Pai, M.M.; Mehbadi, M.; Pai, R.M.; Wu, Y.S. Online and offline communication architecture for vehicular ad-hoc networks using NS3 and SUMO simulators. *J. High Speed Netw.* **2019**, *25*, 253–271.
35. Joe, M.M.; Ramakrishnan, B. WVANET: Modelling a novel web based communication architecture for vehicular network. *Wirel. Pers. Commun.* **2015**, *85*, 1987–2001.
36. Puthal, D.; Mir, Z.H.; Filali, F.; Menouar, H. Cross-layer architecture for congestion control in Vehicular Ad-hoc Networks. In Proceedings of the 2013 International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, NV, USA, 2–6 December 2013; pp. 887–892.
37. Ucar, S.; Ergen, S.C.; Ozkasap, O. Multihop-cluster-based IEEE 802.11 p and LTE hybrid architecture for VANET safety message dissemination. *IEEE Trans. Veh. Technol.* **2015**, *65*, 2621–2636.
38. Liu, Y.C.; Chen, C.; Chakraborty, S. A software defined network architecture for geobroadcast in VANETs. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 6559–6564.
39. Kazmi, A.; Khan, M.A.; Akram, M.U. DeVANET: Decentralized software-defined VANET architecture. In Proceedings of the 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), Berlin, Germany, 4–8 April 2016; pp. 42–47.
40. Venkatramana, D.K.N.; Srikantaiah, S.B.; Moodabidri, J. CISRP: Connectivity-aware intersection-based shortest path routing protocol for VANETs in urban environments. *IET Netw.* **2018**, *7*, 152–161.
41. Zhong, H.; Wen, J.; Cui, J.; Zhang, S. Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET. *Tsinghua Sci. Technol.* **2016**, *21*, 620–629.
42. Silva, A.; Reza, N.; Oliveira, A. Improvement and Performance Evaluation of GPSR-Based Routing Techniques for Vehicular Ad Hoc Networks. *IEEE Access* **2019**, *7*, 21722–21733.
43. Li, W.; Song, W.; Lu, Q.; Yue, C. Reliable congestion control mechanism for safety applications in urban VANETs. *Ad Hoc Netw.* **2020**, *98*, 1–38.
44. Tian, D.; Zhou, J.; Wang, Y.; Sheng, Z.; Xia, H.; Yi, Z. Modeling chain collisions in vehicular networks with variable penetration rates. *Transp. Res. Part C Emerg. Technol.* **2016**, *69*, 36–59.
45. Zhong, H.; Huang, B.; Cui, J.; Xu, Y.; Liu, L. Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks. *IEEE Access* **2018**, *6*, 2241–2250.
46. Rana, K.K.; Tripathi, S.; Raw, R.S. Analytical analysis of improved directional location added routing protocol for VANETs. *Wirel. Pers. Commun.* **2018**, *98*, 2403–2426.
47. Lin, Z.; Tang, Y. Distributed Multi-Channel MAC Protocol for VANET: An Adaptive Frame Structure Scheme. *IEEE Access* **2019**, *7*, 12868–12878.

48. National Institute of Science and Technology. *Secure Hash Standard*; Federal Information Processing Standard (FIPS); National Institute of Science and Technology 180-2: Gaithersburg, MD, USA, 2002.
49. Olaverri-Monreal, C.; Krizek, G.C.; Michaeler, F.; Lorenz, R.; Pichler, M. Collaborative approach for a safe driving distance using stereoscopic image processing. *Future Gener. Comput. Syst.* **2019**, *95*, 880–889.