electronics

MDPI

Article

A Novel Secure Routing Design Based on Physical Layer Security in Millimeter-Wave VANET

Mengqiu Chai [1], Shengjie Zhao [1] and Yuan Liu [2,*]

[1] School of Software Engineering, Tongji University, Shanghai 201804, China; mengqiuchai@tongji.edu.cn (M.C.); shengjiezhao@tongji.edu.cn (S.Z.)
[2] College of Electronic and Information Engineering, Tongji University, Shanghai 201804, China
* Correspondence: tjyuanliu@tongji.edu.cn

Abstract: With the continuous development of millimeter-wave communication technology, new requirements such as ultra-reliability and higher data rates pose new challenges to the security issues of traditional cryptographic encryption in vehicular ad hoc networks (VANET). Physical layer security uses the characteristics of different wireless channels to protect the information security. In this paper, we propose a novel VANET routing mechanism that utilizes physical layer security to improve the secrecy performance, which is compatible with the millimeter-wave vehicular network. Specifically, we design a new secure routing selection factor, the utility function, that takes into account the effects of both secrecy rate and single-hop transmission distance to achieve the hop selection. In addition, we propose a novel routing mechanism and design a waiting mechanism based on the utility function. Compared with the traditional routing algorithms, the greedy perimeter stateless routing (GPSR) and Dijkstra simulation results illustrate that our design achieves superior performance in secrecy performance and dynamic adaptability.

Keywords: millimeter-wave; physical layer security; VANET; 6G; secure routing

Citation: Chai, M.; Zhao, S.; Liu, Y. A Novel Secure Routing Design Based on Physical Layer Security in Millimeter-Wave VANET. *Electronics* **2023**, *12*, 4704. https://doi.org/10.3390/electronics12224704

Academic Editor: Yosef Pinhasi

Received: 6 October 2023
Revised: 12 November 2023
Accepted: 17 November 2023
Published: 19 November 2023

1. Introduction

With the rapid advancement of modern wireless networks, millimeter-wave communication in sixth-generation (6G) networks is required to support higher transmission rates and possess more reliable systems [1–3]. As an important part of the 6G millimeter-wave networks, security has become one of the basic guarantees to support ultra-high data rates, especially in vehicle communications [4–6]. Autonomous vehicles that support millimeter-wave technology are required to provide high data rate services to users in highly diverse traffic environments [7–9]. Vehicular communication networks realize the information sharing between vehicles, roadside infrastructures, pedestrians, and any devices other than the road, which also provides better protection for autonomous vehicles and smart traffic [10,11]. The vehicle-to-vehicle (V2V) communications, vehicle-to-infrastructure (V2I) communications, and vehicle-to-pedestrian (V2P) communications, as well as communications with vulnerable road users (VRUs) and cloud networks, constitute the vehicle-to-everything (V2X) communication network [12]. As a special mobile ad hoc network, vehicular ad hoc network (VANET) plays an increasingly important role in the more and more complex transportation network [13]. In VANET, there are mainly two types of communication units: one is the onboard unit (OBU), and the other is the roadside unit (RSU) [14,15]. In addition, there are also traffic cloud nodes, servers, and base stations in the vehicle network. Vehicles can perceive road conditions in real time and broadcast road information through the traffic management platform [16], helping neighboring car nodes obtain road traffic information for information sharing. Moreover, the vehicles can obtain relevant roadside traffic service auxiliary information by interacting with roadside nodes. Through information transmission with the traffic cloud center node, it can complete applications, such as big data computing [17]. Due to the characteristics of vehicle

networking, the vulnerability of network links brought by the rapid movement of vehicles, and the increasing amount of vehicle interaction data, the security of information becomes more and more important in vehicular networks [16]. The demand for vehicular networks has gradually changed from simply improving travel efficiency to multi-level requirements, such as traffic information, social information, and user personal information sharing. With the development and application of 6G, the volume of data will increase exponentially in the vehicular networks. If the security in vehicular networks can not be guaranteed, it will cause an immeasurable impact. Therefore, in 6G vehicle networking, security is a very important issue [18].

VANET has the main features of MANET, while it also has some unique characteristics. As a node in the network, the vehicle moves randomly and dynamically, which makes the link between vehicles fragile and vulnerable [19,20]. When applying the traditional internet protocol stack, the network characteristics of VANET lead to security vulnerabilities and hidden dangers between different layers [21]. At the same time, wireless communication has the characteristic of broadcasting, which makes the information transmission security in the entire communication system indefensible under the existence of eavesdroppers [22–25]. Therefore, many studies focus on the issue of the security of VANET. Public key infrastructure (PKI) is considered a feasible mechanism to protect VANET. However, PKI cannot provide specific security requirements, such as location privacy, effective authentication, fair revocation, etc. Wasef et al. [26] introduced complementary security mechanisms to guarantee the security requirements in the PKI. Some researchers study using the physical attributes of the V2V channels to generate the cryptographic keys. The problem of solving the non-reciprocal propagation difference is studied in the process of generating the highly random and symmetric key in the physical layer characteristics of the V2V propagation channel [27]. The private key generator as a third trusted entity responsible for the generation and allocation of private keys to enhance the VANET security is employed in the identity-based signature (IBS) scheme [28]. To eliminate the management of certificates and solve the escrow problem in the VANET system, the certificateless signature is proposed to provide a reliable identity authentication [29]. The 5G-VANET security group communication based on software-defined network technology (SDN) is studied to solve the main security challenges in distributed and centralized networks [30]. All the aforementioned existing methods are compared in Table 1.

Physical layer security guarantees the promising security of the system by means of the unique characteristic of the wireless channel, which is a significant complement of traditional cryptographic encryption methods [31–36]. In recent years, some attention has been attracted to introducing physical layer security to vehicular networks. In [37], the security of the system is obtained by using symmetric key cryptography techniques, while the key security is achieved using a physical layer security mechanism. In multi-hop networks, security can be achieved by enhancing physical layer security technologies, such as cooperative interference and cooperative relay [38]. In terms of the random distribution of eavesdroppers [39], addresses the issue of maximizing confidentiality by jointly designing the wiretap code and routing, subject to the secrecy outage probability (SOP) constraint, which finally solves the secure routing problem with the improved Bellman–Ford algorithm. The work in [40] has studied optimal secure routing based on the secrecy connectivity probability (SCP) in multi-hop ad hoc networks with randomize-and-forward relaying in the presence of inhomogeneous eavesdropper clusters. In ref. [41], they proposed a routing algorithm that considers the cross-layer approach of using physical layer and network layer information to effectively support QoS transport.

Table 1. Comparison of the existing methods.

Reference	Scheme	Characteristic	Limitation
[26]	Public Key Infrastructure	Identity authentication; Key management	The system is complex and can not guarantee security once the central infrastructure is attacked.
[27]	Symmetric Cryptography	High efficiency; Lower overhead	The key management is vulnerable and lack of non-repudiation property.
[28]	Identity-Based Signature	Certificate free; Identity as Public Key	The association between identity and the public key has to be trusted.
[29]	Certificateless Signature	Enhanced security; No certificate dependency	This scheme introduces additional complexity.
[30]	Group Signature	Selective Disclosure; Non-repudiation	Revoking the signing privileges of an individual member without impacting the entire group is a challenge.

Contributions and Paper Organization

Considering the existence of eavesdropping nodes in the vehicular network, this paper proposes a secure routing mechanism based on physical layer security. To the best of the authors' knowledge, this is the first instance in which a routing mechanism has been integrated with physical layer security. Different from the existing routing mechanisms for VANET, which are mainly based on the reliability of the link, the proposed routing mechanism designs a utility function considering both the secrecy performance of the link and the transmission performance. Moreover, the routing mechanism considers the common road traffic conditions and designs corresponding strategies. Compared with the traditional routing mechanisms, the simulation results verify the secrecy performance of our routing mechanism. The main contributions of this article can be summarized as follows:

- Corresponding to the security requirements of the 6G millimeter-wave networks, we studied the secure routing mechanism of the vehicular network which is an important part of the 6G millimeter-wave-integrated network. In order to improve the secrecy performance of the VANET, we utilize physical layer security to design a utility function that takes into account the secrecy performance and transmission performance as the selection principle for each hop in VANET.
- Based on the designed utility function, we further propose a new secure routing mechanism for the VANET. It takes into account the common routing scenarios. In view of the hop selection not meeting the security requirement, a corresponding waiting mechanism is designed to ensure the security of routing under various complex situations.
- Simulation results verify the improvement of the proposed VANET routing mechanism in secrecy performance. Compared with the traditional routing algorithms, Dijkstra and greedy perimeter stateless routing (GPSR),whether in the case of a large number of vehicles, complex topology, or different speed ranges, the secrecy performance of the proposed secure routing mechanism is significantly improved without the cost of high transmission delay.

The rest of this paper is organized as follows. In Section 2, the system model and the design of the utility function utilizing physical layer security are introduced. Section 3 provides the proposed secure routing mechanism and waiting mechanism considering common situations in VANET. Section 4 demonstrates the numerical results. Section 5 concludes the whole paper.

2. System Model

As illustrated in Figure 1, we consider a dynamical secure routing scenario in VANET where one vehicle acts as an eavesdropper denoted by v_e and the legitimate vehicles are denoted by $v_n, 1 < n \leq N$. N denotes the number of all legitimate vehicles. All lanes are

divided into two directions, and vehicles follow the corresponding prescribed directions in their respective lanes. The speed of all vehicles is within a given range. The source vehicle v_1 needs to transmit the message to the destination vehicle v_N. Due to the rapid attenuation of the mmWave signal, the limited coverage is denoted by R, and the message needs to be transmitted in multiple hops from the source vehicle to the destination vehicle where each hop is denoted by $l_k, 1 < k \leq K$, and K denotes the total number of hops in the routing process. Taking l_1 into consideration, the neighbor nodes of v_1 is $v_2 \sim v_6$. Some traditional mechanisms in VANET, such as GPSR [12] and Dijkstra, tend to choose v_4 as the next hop, which is the closest node to v_N. However, from the perspective of security, v_4 is also close to v_e, which means that the secrecy performance can not be guaranteed totally. Therefore, if the VANET exists in the eavesdropping node, directly selecting the farthest node does not guarantee the security of the network, which enlightens us that only considering the distance in the routing process is limited to ensuring the security of the routing process.

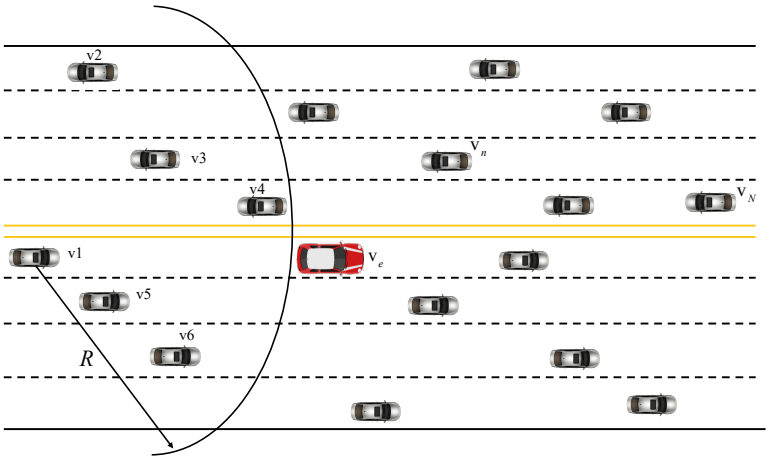

Figure 1. The secure routing scenario in vehicular ad hoc networks.

Utility Function

As one of the main characteristics of VANET, rapid changes in topological structure, which leads to unstable links, can make the wireless channel unique. This creates a natural advantage for the physical layer security. Therefore, we consider combining physical layer security and the traditional routing indicator to design a utility function ε that can ensure both the secrecy performance and the transmission performance,

$$\varepsilon_{ij} = C_{S_{ij}}^{\alpha} d_{ij}^{\beta}, \tag{1}$$

where ε_{ij} denotes the utility function between vehicle v_i and v_j; $C_{S_{ij}}$ denotes the secrecy capacity of the channel between v_i and v_j; d_{ij} denotes the distance between v_i and v_j; α denotes the weight of secrecy capacity; and β denotes the weight of the distance. α and β can be adjusted flexibly, $\alpha, \beta \in (0, 1)$, $\alpha + \beta = 1$. The channel capacity C_{ij} between v_i and v_j can be described as

$$C_{ij} = \log_2\left(1 + \frac{P_t h_{ij} h_{ij}^*}{\sigma^2}\right). \tag{2}$$

The channel capacity C_{ie} between v_i and v_e can be formulated as

$$C_{ie} = \log_2\left(1 + \frac{P_t h_{ie} h_{ie}^*}{\sigma^2}\right). \tag{3}$$

In the two formulas above, P_t denotes the transmit power of all vehicles, h_{ij} denotes the channel between v_i and v_j, h_{ie} denotes the channel between v_i and v_e, and σ denotes the variance of the additive Gaussian white noise. The secrecy capacity $C_{S_{ij}}$ is

$$C_{S_{ij}} = \max\{C_{ij} - C_{ie}, 0\}. \tag{4}$$

By examining Equation (4), it can be observed that the maximum value of the secrecy capacity is attained when C_{ie} equals zero. Therefore, the maximum secrecy capacity can be achieved when the channel capacity C_{ie} between v_i and v_e is small enough, which can be expressed as $C_{S_{ij}}^{\max} \approx C_{ij}$.

Following the utility function, the selected next node of this hop is

$$j^* = \arg\max_j \{\varepsilon_{ij}\}. \tag{5}$$

3. Proposed Secure VANET Routing Mechanism

On the basis of the proposed utility function, in this section, we design a secure vehicular network routing mechanism to improve the secrecy performance of the transmission process. The routing mechanism takes into account common vehicle situations. In addition, according to the requirement of utility function, there may be no alternative route choice, and we design a specific waiting mechanism to deal with this situation. The flowchart of the proposed routing mechanism is shown in Figure 2.

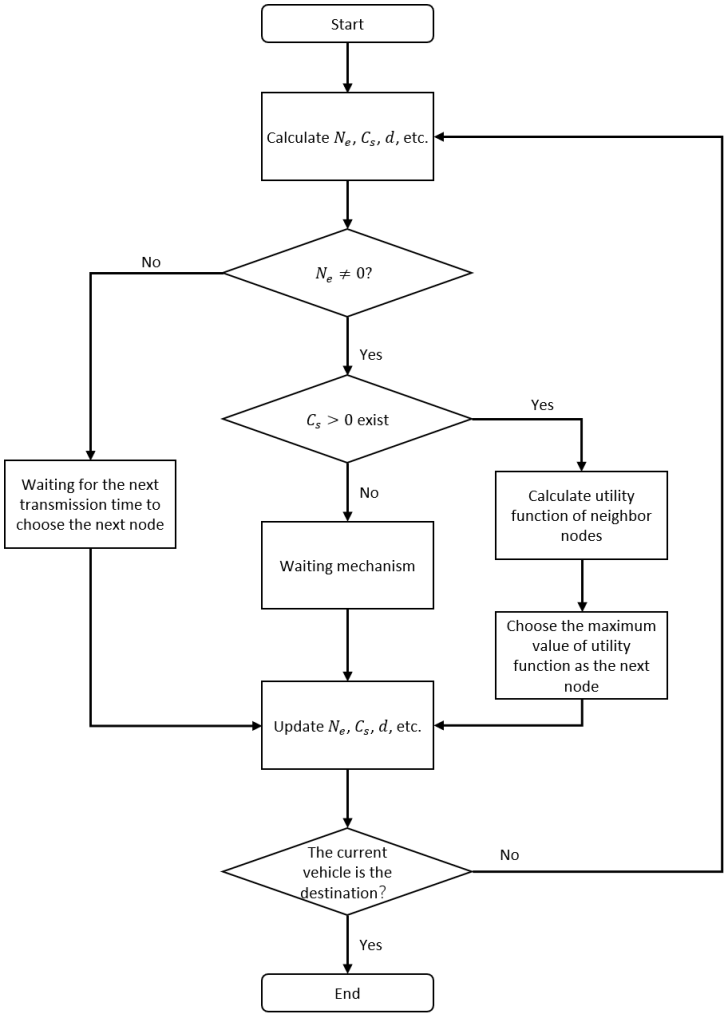

Figure 2. The flowchart of the secure vehicular ad hoc network (VANET) routing mechanism.

3.1. Secure Routing Transmission

The critical component of the routing mechanism utilizes the characteristics of different wireless channels to protect the security from the eavesdropping vehicle. We assume that every vehicle knows its own position information and the global information is available for the current vehicle to set up its routing.

According to the distribution of vehicles on the two-direction-multi-lane straight road and the consideration of the design of the utility function, we denote the number of the current vehicle in a radius of R as N_e and the vehicular situation of the routing mechanism can be roughly divided into the following situations.

If there is no neighbor vehicle in a radius of R, the message will remain in the c vehicle. After a fixed time interval t_i, the current vehicle will implement selection for the next hop again. When there is at least one neighbor vehicle with a secrecy capacity greater than zero in the radius of R, the current vehicle calculates the values of the utility function and selects the maximum value of the neighbor vehicles as the next node in the routing process. After the completion of this hop, the positions of the vehicles and all information in the routing process update and wait for the next t_i to select the next hop. There remains another situation in which the number of neighbor vehicles is greater than zero while none of them has the value of secrecy capacity greater than zero. In order to enable the proposed routing mechanism to continue to work in this case, we design a waiting mechanism that helps the current vehicle search for a potential neighbor vehicle as the next hop. The design of secure routing is shown in Algorithm 1.

Algorithm 1 The proposed secure routing mechanism

```
Initialize: Generate the speed and position of all vehicles randomly. Set parameter α, β.
for the current vehicle is not the destination v_N do
  if N_e ≠ 0 then
    calculate d, C_s;
    if N_e with C_s ≥ 0 then
      calculate utility function of neighbor nodes;
      choose the maximum value of utility function as the next node;
    else
      entering the 'waiting mechanism';
    end if
  else
    waiting for the next transmission time to choose the next node;
  end if
  updating the routing table;
end for
```

3.2. Waiting Mechanism

As for the situation with neighbor vehicles around the current vehicle, none of the neighbor vehicles with secrecy capacity greater than zero waiting until the next selected time will seriously delay the overall transmission time. Therefore, we propose a waiting mechanism for this situation.

Specifically, we set a waiting time window t_w and a threshold of the total waiting time T. Based on the location information and vehicle speed information at the beginning of the current waiting time window, predict the location and secrecy capacity of neighbor vehicles after the current waiting time window to determine whether there are potential selection vehicles $N_e^{'}$ that meet the secure requirement. If there are neighbor vehicles that meet the secure requirement, the vehicle with the largest utility function value is selected as the next vehicle and ends the waiting mechanism. If there is no neighbor vehicle that meets the secure requirements, the waiting time window is extended by an exponential of 2. If the total waiting time does not exceed the wait time threshold at this point, it continues with the same operation. If the waiting time threshold is exceeded, the message remains in the

current vehicle and the waiting mechanism is ended. The design of the waiting mechanism is represented in Algorithm 2.

Algorithm 2 Design of waiting mechanism

Initialize: the first waiting time window t_{w1}, threshold of the total waiting time T.
for the total waiting time < T **do**
  predict location of neighbor nodes based on the situation at the beginning of the current waiting time window;
  if $N_e^{'}$ *with* $C_s \geq 0$ **then**
    calculate utility function of neighbor nodes;
    choose the maximum value of the utility function as the next vehicle;
    break;
  else
    increase the next waiting time window by 2 times the index;
  end if
end for

3.3. Complexity Analysis

In order to better evaluate the proposed Algorithms 1 and 2, we analyze their complexities in this section. For Algorithm 1, without considering the waiting mechanism, in a single-loop process assuming the current vehicle is not the destination and $N_e \neq 0$, the computational complexity of calculating a single C_S is $2N_e + 1$, $d = N_e$. In the worst-case scenario, the information needs to be transmitted through all vehicles to reach the destination. Therefore, the overall complexity of Algorithm 1 is $N(2N_e + 1)$. As for Algorithm 2, assuming that all vehicles can find the next vehicle within the total waiting time T, the total complexity of Algorithm 2 with the first waiting time window t_{w1} is $N(log_2(\frac{T+t_{w1}}{2t_{w1}}) + 1)(2N_e + 1)$.

4. Simulations and Discussion

In this section, we present simulation results to demonstrate the secrecy performance of our proposed secure routing mechanism for VANET. Each transmission process from v_1 to v_N consists of several single loops. In order to ensure the reliability of the whole transmission, we choose the minimum secrecy capacity of all selected hops to evaluate the secrecy performance of each routing process. All simulation results are obtained by taking the average over 1000 Monte Carlo simulations in MATLAB R2021a. All vehicles are randomly distributed in an 8-lane road environment with a total width of 28 m. The width of each lane is equal with four lanes in one direction and the other four lanes in the opposite direction. Considering the practical movement of the vehicle, we choose the default vehicle speed as 40–60 km/h which can showcase the change of topology of VANET. More detailed parameters are summarized in Table 2.

Table 2. Simulation parameters.

Parameters	Value
Simulation times	1000
Length of lane	1000 m
Range of communication	200 m
Total waiting time threshold	65 ms
Default speed range	40–60 km/h
High car speed	80–120 km/h
Weight in utility function α	0.1–0.9
Weight in utility function β	0.1–0.9
Initial waiting time window	130 µs
Bandwidth	10 MHz
Transmit power	10 dBm
AWGN Power σ^2	−174 dBm
Number of vehicles	20/40/60/80/100

4.1. Secrecy Performance

In the designed utility function, the parameter corresponding to secrecy capacity is α, the parameter corresponding to the distance between single hops is β, and the sum of α and β is 1. The larger the value of α, the greater the influence of secrecy capacity in routing selection, and the smaller the influence of distance effect. This leads to the utility function tending to select the closer node with better secrecy performance for transmission when selecting the next hop vehicle. The total number of hops may increase, and the overall transmission delay becomes larger. Conversely, if the value of α becomes smaller, the distance between the two vehicles in the routing hop selection will be more important and the overall transmission delay will be reduced. However, the secrecy capacity of the communication system will also decline, which will lead to a significant increase in the risk of a vehicular network being eavesdropped. In the following, we analyze the secrecy performance of the vehicular network under different weights in the utility function.

Figure 3 showcases the secrecy performance when $\alpha = 0.5$, i.e., the security factor and the transmission factor in the utility function are equally weighted. It can be observed that with the increment of the number of vehicles, the value of the secrecy capacity is increasing significantly. This is because the more the number of vehicles, the smaller the distance between two adjacent vehicles and the more next-hop vehicles that can be selected within the communication range, which leads to the greater value of the utility function. At the same time, we can notice that when the number of vehicles increases from 20 to 40, the secrecy capacity increases significantly. When the number of vehicles changes from 40 to 80, the secrecy capacity increases slowly. Moreover, there is little difference between the secrecy capacity of 80 vehicles and that of 100 vehicles, which indicates that the secrecy performance of the vehicular network reaches a stable value when the weight of α is small.

Figure 4 illustrates the secrecy performance when $\alpha < 0.5$. As expected, for each specified number of vehicles, as the weight of α increases, the secrecy capacity increases significantly. Additionally, as the number of vehicles continues to increase, the four curves all show a gradually increasing trend. Specifically, for the curve of $\alpha = 0.1$, $\beta = 0.9$, when the number of vehicles is 20, 40, and 60, the change in secrecy capacity is not significant. Until the number of vehicles is 80 and 100, the secrecy capacity shows little improvement. This illustrates that when the weight of α is too low in the utility function, it is difficult to significantly improve the secrecy performance of the network even with the increase of the number of vehicles in the network. In comparison, the curve of $\alpha = 0.2$ and $\beta = 0.8$ shows a clear upward trend. When the number of vehicles is 60, the curve can reach good secrecy performance. As the number of vehicles continues to increase, the secrecy capacity shows no significant change. For the curve of $\alpha = 0.3$ and $\beta = 0.7$, when the number of vehicles is 80, the network achieves a high secrecy performance stably. For the curve of $\alpha = 0.4$ and $\beta = 0.6$, when the number of vehicles reaches 40, its secrecy capacity has reached a stable and high level. It indicates that the larger the weight of α in the utility function, the more stable the secrecy capacity tends to be when $\alpha < 0.5$ and the number of vehicles is smaller.

Figure 5 presents the secrecy performance when $\alpha > 0.5$. We can find that the changing trend of secrecy capacity in Figure 5 is significantly greater than that in Figure 4. This shows that when the weight of the secrecy capacity in the utility function exceeds 0.5, the secure performance of the selected routing process changes tremendously. Especially, when $\alpha = 0.9$ and $\beta = 0.1$, the secrecy capacity of 100 vehicles can be twice as high as that of 20 vehicles. Moreover, the growth trend of the two curves, $\alpha = 0.6$ and $\alpha = 0.7$, is roughly the same. The value of the two curves, $\alpha = 0.7$ and $\alpha = 0.8$, are close. When the weight of α increases to 0.9, the secrecy capacity varies greatly and grows rapidly. We can find that when α reaches a higher value, the utility function achieves great performance in achieving secure VANET.

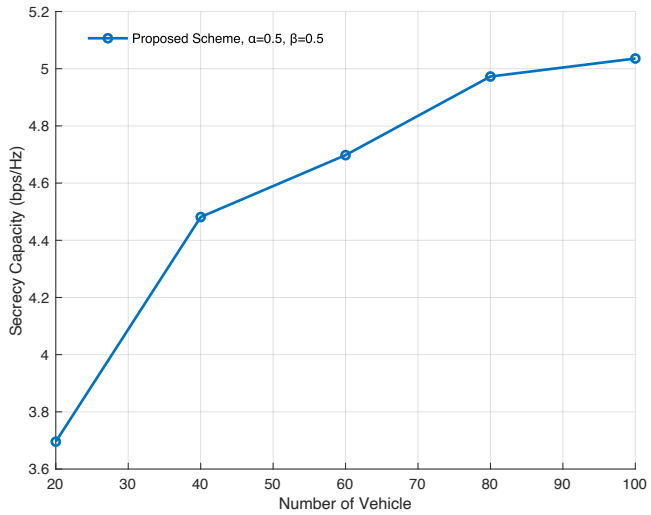

Figure 3. Secrecy capacity of the proposed secure routing mechanism when $\alpha = \beta = 0.5$.

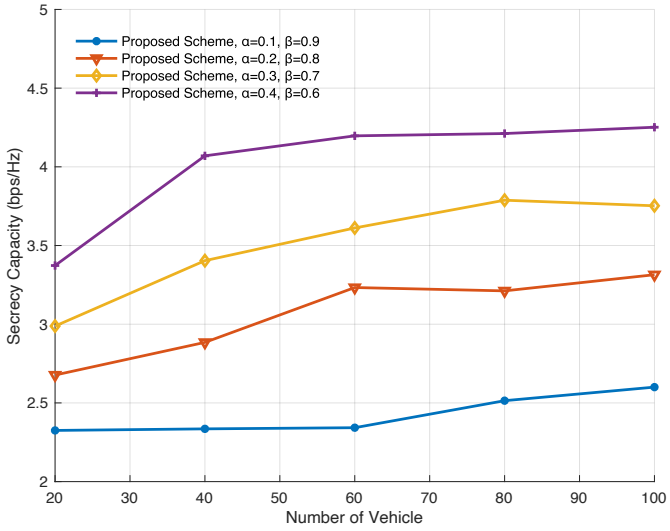

Figure 4. Secrecy capacity of the proposed secure routing mechanism when $\alpha < 0.5$.

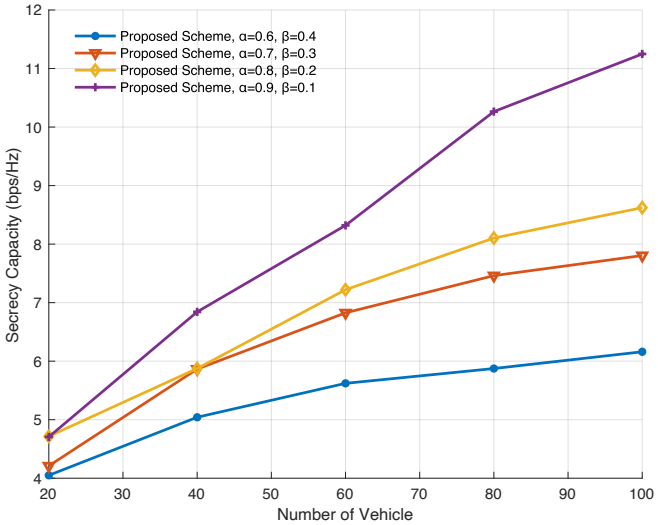

Figure 5. Secrecy capacity of the proposed secure routing mechanism when $\alpha > 0.5$.

4.2. Transmission Delay

In the previous subsection, we analyze the secrecy performance of the proposed secure VANET routing mechanism. However, if the maximum secrecy performance is blindly pursued, selecting the nearest vehicle for each hop will result in a long transmission delay, which also can significantly affect the transmission performance in the vehicular network. In this subsection, we analyze the overall transmission delay of the proposed routing mechanism.

Figure 6 shows the overall transmission delay of the proposed secure routing mechanism when α ranges from 0.1 to 0.9. We can find that when α ranges from 0.1 to 0.6, there is no obvious difference in the overall transmission delay under different vehicle numbers. The transmission delay of $\alpha = 0.7$ increases slightly with the number of vehicles and is slightly higher than α ranging from 0.1 to 0.6. When $\alpha = 0.8$, $\beta = 0.2$, and $\alpha = 0.9$, $\beta = 0.1$, the overall transmission delay is significantly higher than other situations when the number of vehicles is larger. This is because when the number of vehicles is larger, there are more available vehicles, and the closer vehicle is selected in the routing process. With the number of selected vehicles increasing, the time for routing and waiting at each vehicle increases, which causes a high overall transmission delay.

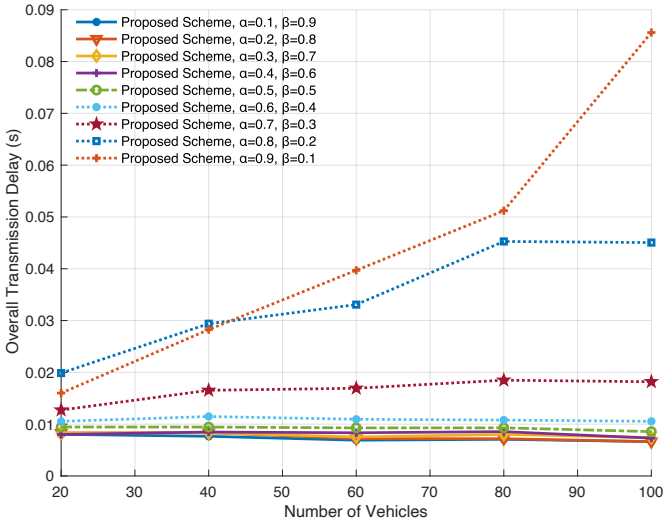

Figure 6. Overall transmission delay of the proposed secure routing mechanism.

4.3. Comparison with Traditional Routing Mechanism

The basic performance of the designed utility function and proposed routing mechanism is shown in the above subsections. In this subsection, we compare and analyze the proposed secure routing mechanism with two traditional routing mechanisms, Gijkstra and GPSR. Based on the above analysis, we select three representative curves of our proposed mechanism, $\alpha = 0.3$, $\alpha = 0.5$, and $\alpha = 0.7$, to make a comparison with the two traditional routing mechanisms.

Figures 7 and 8 present the secrecy capacity and overall transmission delay under the proposed routing mechanisms, Dijkstra algorithm and GPSR algorithm. The shortest path planning algorithm, Dijkstra, plans the routing selection based on the static distribution of vehicles initially without considering the mobility of the vehicles. Therefore, as the number of vehicles increases, it shows a gradual decline in secrecy capacity. This indicates that when the number of vehicles increases, the topology structure of each vehicle node changes significantly as the routing process continues and Dijkstra's dynamic adaptability is poor. Therefore, for the network with dynamic structures, the Dijkstra routing mechanism does not have any advantages in secure transmission. Since each hop of the GPSR algorithm is selected according to the neighbor nodes in the current environment of the specific vehicle, it has better dynamic adaptability than Dijkstra. Therefore, with the increase in the number of vehicles, the secrecy capacity of the GPSR algorithm remains stable, and

its secrecy capacity is higher than that of Dijkstra. Compared with Dijkstra and GPSR, the three curves of our proposed routing mechanism when α = 0.3, 0.5, and 0.7 achieve a significant increase in secrecy capacity. When α = 0.3, the secrecy capacity of our proposed algorithm is higher than the traditional mechanisms. When α = 0.5 and 0.7, the secrecy capacity can be greatly improved. As the number of vehicles increases, the secrecy capacity of our proposed routing mechanism can be significantly promoted, which is not possible with traditional algorithms.

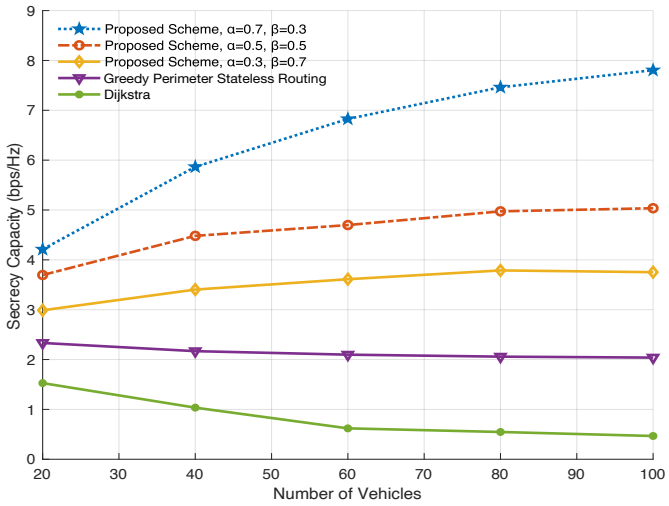

Figure 7. Secrecy performance comparison of Gijkstra, GPSR, and the proposed mechanism.

By comparing Figures 7 and 8, we can find that the overall transmission delay is small because Dijkstra and GPSR tend to choose the farther vehicle in fewer hops during the routing. However, since we consider the secrecy factor as well as the transmission distance when designing the utility function, the two curves of α = 0.3 and α = 0.5 are not much different from Dijkstra and GPSR in terms of overall transmission delay. Especially the curve of α = 0.3 and β = 0.7, it has a slight difference with Dijkstra and GPSR in terms of transmission delay. However, it achieves much higher secrecy capacity than Dijkstra and GPSR, which illustrates the advantages of our proposed utility function and routing design where it can balance the transmission latency and secure performance flexibly. Moreover, the curve of α = 0.5 is not much longer in terms of transmission delay, but the secrecy performance is much better than that of Dijkstra and GPSR. When α = 0.7, the designed routing mechanism achieves a much higher secrecy capacity than that achieved by GPSR and Dijkstra. However, at this time, the overall transmission delay has increased significantly. It illustrates that the choice of weights in the utility function is important when our design comes to the practical application. Otherwise, the secrecy performance may be improved but the transmission delay is too long. It is worth noting that the increase in transmission delay does not cause calculation errors.

4.4. Performance in High-Speed VANET

In the previous subsections, the speed of the vehicles in VANET ranges from 40 to 60 km/h. In practice, the speed of the vehicles may be much higher and the topology of the VANET changes faster. Therefore, it is worth studying the performance of the proposed utility function and secure routing mechanism in the high-speed situation ranging from 80 to 120 km/h.

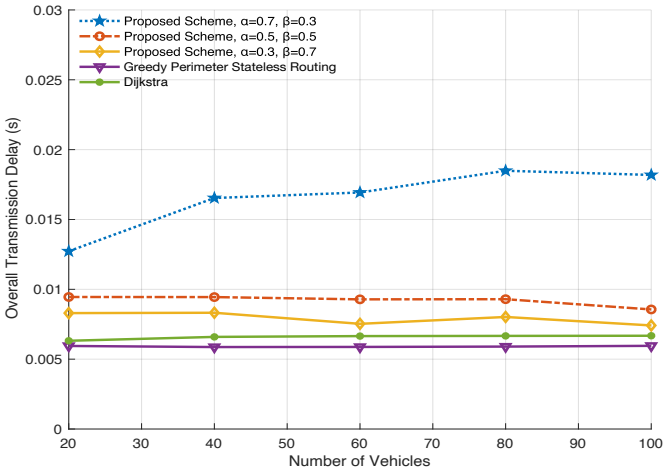

Figure 8. Overall transmission delay comparison of Gijkstra, GPSR, and the proposed mechanism.

First, we consider the secrecy and transmission performance of the proposed VANET routing mechanism. Figures 9–11 show the secrecy capacity and overall transmission delay of the proposed routing scheme with $\alpha = 0.3$, $\beta = 0.7$, $\alpha = 0.5$, $\beta = 0.5$, and $\alpha = 0.7$, $\beta = 0.3$ at different vehicle speeds. As shown in the left figure of Figure 9, when the number of vehicles in VANET increases, the secrecy capacity of both medium-speed and high-speed situations increases, but the secrecy capacity of high-speed vehicle networks increases more slowly. This is because, in the utility function at this time, the factor of transmission distance occupies the main influence in routing hop selection. Combined with the figure on the right, the overall transmission delay in high-speed situations is generally lower than that in medium-speed situations. When the number of vehicles increases, the topology of the VANET changes rapidly at high speeds, and the transmission delay also increases compared with that at medium speeds.

As shown in the left figure of Figure 10, the growth trend and specific values of the two curves are roughly the same, while the overall transmission delay in the right figure is also not much different under two speed situations. Only when the number of vehicles is 20, the secrecy capacity of high-speed moving vehicles is slightly higher than the medium speed. This shows that the utility function designed and the proposed routing mechanism have great performance in both medium and high-speed motion when the two indexes in the utility function are equally affected.

In Figure 11, when the number of vehicles is 20 and 100, the secrecy capacities almost overlap under the two-speed conditions. When the number of vehicles is 40, 60, and 80, the secrecy capacities decrease slightly under the high-speed condition while it remains relatively high. It illustrates that the VANET can maintain high stability with the proposed design. When the number of vehicles is 40, the transmission delay in the high-speed situation is slightly higher than that in the low-speed situation. By comparing Figures 9–11, it demonstrates that the proposed routing mechanism can maintain stability and high secrecy performance under the condition of high-speed VANET.

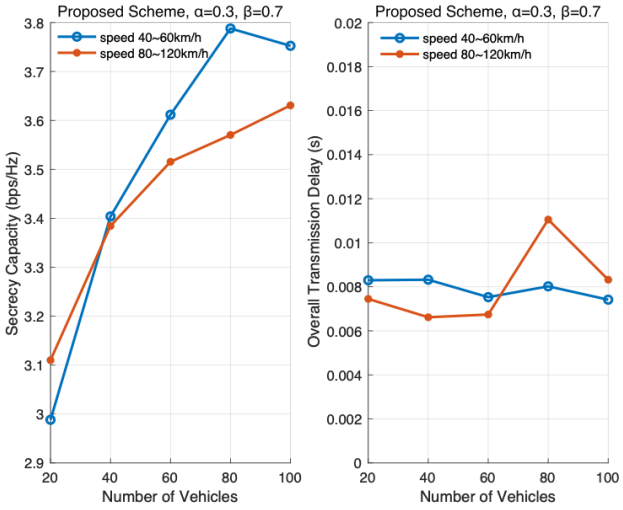

Figure 9. Secrecy performance of the proposed mechanism with $\alpha = 0.3$, $\beta = 0.7$ at different vehicle speeds.

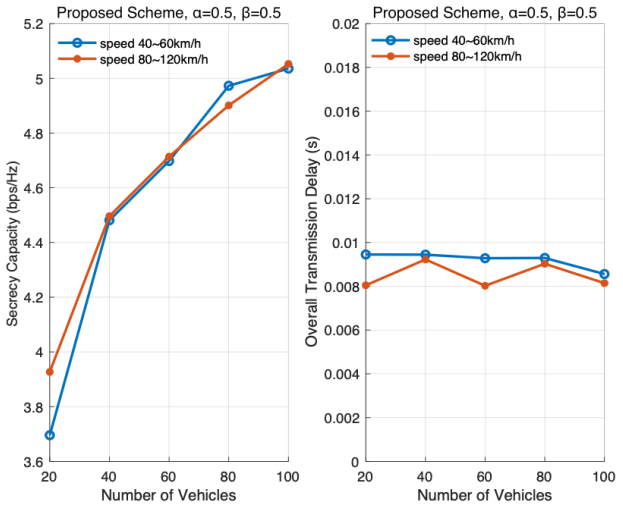

Figure 10. Secrecy performance of the proposed mechanism with $\alpha = 0.5$, $\beta = 0.5$ at different vehicle speeds.

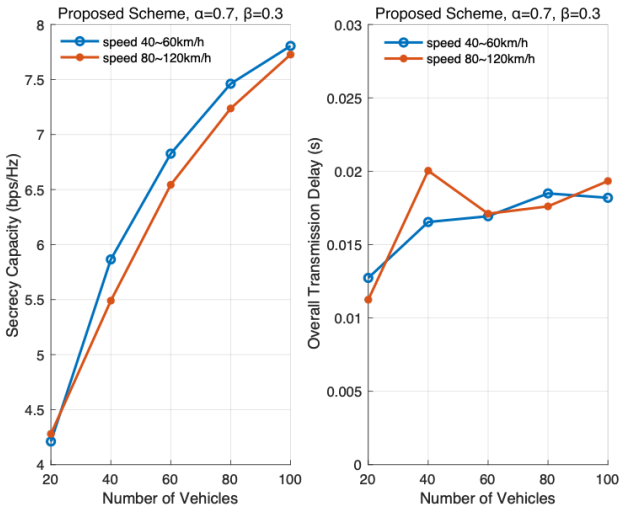

Figure 11. Secrecy performance of the proposed mechanism with $\alpha = 0.7$, $\beta = 0.3$ at different vehicle speeds.

Figures 12 and 13 present two classical routing mechanisms, Dijkstra and GPSR, at different vehicle speeds. From Figure 12, we find that the secrecy capacity achieved by the Dijkstra algorithm decreases significantly as the number of vehicles increases in both medium and high-speed situations. Moreover, the value of secrecy capacity achieved by Dijkstra is very low for any number of vehicles. At each specific number of vehicles, the difference in the secrecy capacity is not very big. It illustrates the poor secure performance and bad dynamic adjustment of Dijkstra. The overall transmission delay remains almost the same at different speed situations and only slightly increases with the increase in the number of vehicles without significant changes. From Figure 13, it can be seen that the secrecy capacity achieved by the GPSR algorithm also decreases as the number of vehicles increases. For the curve ranging from 80 to 120 km/h, the value of the secrecy capacity is smaller and the decline is greater than that of the curve ranging from 40 to 60 km/h. There is not much difference in overall transmission delay under two different vehicle speeds and different numbers of vehicles. By comparing Figures 9 and 13, we can find that Dijkstra achieves the worst secrecy performance. When the VANET topology is complex and the vehicle speed is fast, the performance will further deteriorate. This is because the Dijkstra algorithm generates the shortest path for node selection based on the node distribution diagram at the initial moment, and does not adapt to subsequent changes. Therefore, it does not have good adaptability to high-speed situations. Although the GPSR algorithm selects hop by hop, it does not have good adaptability to complex VANET topology structures and high-speed situations. However, the proposed routing mechanism and designed utility function can achieve stable and great performance in the VANET with complex topology and high-speed moving situations.

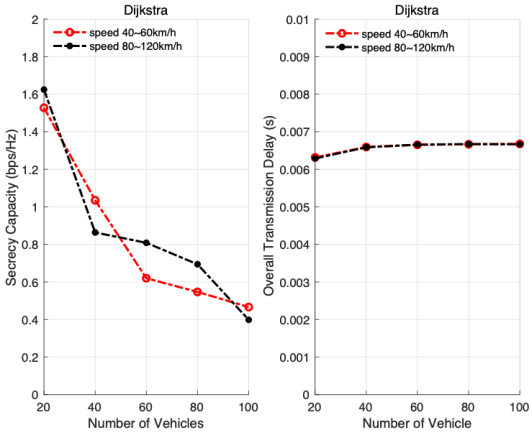

Figure 12. Secrecy performance of the Dijkstra algorithm at different vehicle speeds.

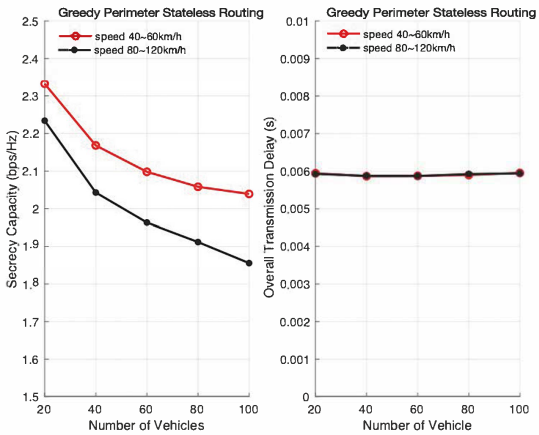

Figure 13. Secrecy performance of the GPSR algorithm at different vehicle speeds.

5. Conclusions

In this paper, we study a secure routing mechanism that can effectively improve the secrecy performance of vehicular networks in millimeter-wave communication vehicle networks. Specifically, we utilize physical layer security to propose a utility function to select routing vehicles, which considers both secrecy capacity and transmission distance between vehicles. Moreover, we design the corresponding routing mechanism and a waiting mechanism considering common situations and the secrecy capacity of potential vehicles. The simulation results show that the proposed routing mechanism can maintain better secrecy performance than Dijkstra and GPSR in the case of complex dynamic topology and high-speed ranges. Additionally, due to the flexible weight adjustment of the utility function, the routing mechanism can meet different secrecy requirements of VANET, which has broad application prospects. In the future, our focus will be on integrating the proposed mechanism into more practical scenarios and exploring safer mechanisms by combining it with novel technologies, such as intelligent reflecting surfaces and unmanned aerial vehicles.

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

Funding: This work was supported in part by the National Key R&D Program of China 2019YFB2102300 and 2019YFB2102301, in part by National Natural Science Foundation of China under Grant 61936014, in part by Shanghai Municipal Science and Technology Major Project No. 2021SHZDZX0100, in part by Shanghai Science and Technology Innovation Action Plan Project 22511105300, and in part by Fundamental Research Funds for the Central Universities.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

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

References

1. Jiang, H.; Mukherjee, M.; Zhou, J.; Lloret, J. Channel Modeling and Characteristics for 6G Wireless Communications. *IEEE Netw.* **2021**, *35*, 296–303. [CrossRef]
2. Hong, W.; Jiang, Z.H.; Yu, C.; Hou, D.; Wang, H.; Guo, C.; Hu, Y.; Kuai, L.; Yu, Y.; Jiang, Z.; et al. The Role of Millimeter-Wave Technologies in 5G/6G Wireless Communications. *IEEE J. Microwaves* **2021**, *1*, 101–122. [CrossRef]
3. Liu, Y.; Han, F.; Zhao, S. Flexible and Reliable Multiuser SWIPT IoT Network Enhanced by UAV-Mounted Intelligent Reflecting Surface. *IEEE Trans. Reliab.* **2022**, *71*, 1092–1103. [CrossRef]
4. Jiang, H.; Zhang, Z.; Dang, J.; Wu, L. A Novel 3-D Massive MIMO Channel Model for Vehicle-to-Vehicle Communication Environments. *IEEE Trans. Commun.* **2018**, *66*, 79–90. [CrossRef]
5. Wang, C.; Wang, H.M. Physical Layer Security in Millimeter Wave Cellular Networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 5569–5585. [CrossRef]
6. Liu, Y.; Zhao, S.; Han, F.; Chai, M.; Jiang, H.; Zhang, H. Data Collection for Target Localization in Ocean Monitoring Radar-Communication Networks. *Remote Sens.* **2023**, *15*, 5126. [CrossRef]
7. Fan, B.; Tian, H.; Zhu, S.; Chen, Y.; Zhu, X. Traffic-Aware Relay Vehicle Selection in Millimeter-Wave Vehicle-to-Vehicle Communication. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 400–403. [CrossRef]
8. De Mendoza, C.R.; Cervelló-Pastor, C.; Sallent, S. Optimal Resource Placement in 5G/6G MEC for Connected Autonomous Vehicles Routes Powered by Deep Reinforcement Learning. In Proceedings of the 2023 IEEE 48th Conference on Local Computer Networks (LCN), Daytona Beach, FL, USA, 2–5 October 2023; pp. 1–4.
9. Chai, M.; Zhao, S.; Liu, Y.; Ding, F.; Sun, H.; Jiang, R. Intelligent Reflecting Surface-Assisted Full-Duplex UAV-Based Mobile Relay Communication. In *Mobile Multimedia Communications. Proceedings of the 14th EAI International Conference, Mobimedia 2021, Virtual Event, 23–25 July 2021*; Xiong, J., Wu, S., Peng, C., Tian, Y., Eds.; Springer: Cham, Switzerland, 2021; pp. 212–223.
10. Bagheri, H.; Noor-A-Rahim, M.; Liu, Z.; Lee, H.; Pesch, D.; Moessner, K.; Xiao, P. 5G NR-V2X: Toward Connected and Cooperative Autonomous Driving. *IEEE Commun. Stand. Mag.* **2021**, *5*, 48–54. [CrossRef]

11. Chen, S.; Hu, J.; Shi, Y.; Peng, Y.; Fang, J.; Zhao, R.; Zhao, L. Vehicle-to-Everything (v2x) Services Supported by LTE-Based Systems and 5G. *IEEE Commun. Stand. Mag.* **2017**, *1*, 70–76. [CrossRef]
12. Noor-A-Rahim, M.; Liu, Z.; Lee, H.; Khyam, M.O.; He, J.; Pesch, D.; Moessner, K.; Saad, W.; Poor, H.V. 6G for Vehicle-to-Everything (V2X) Communications: Enabling Technologies, Challenges, and Opportunities. *Proc. IEEE* **2022**, *110*, 712–734. [CrossRef]
13. Soni, G.; Chandravanshi, K. A Novel Privacy-Preserving and Denser Traffic Management System in 6G-VANET Routing Against Black Hole Attack. In *Sustainable Communication Networks and Application: Proceedings of ICSCN 2021*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 649–663.
14. Liao, L.; Zhao, J.; Hu, H.; Sun, X. Secure and Efficient Message Authentication Scheme for 6G-Enabled VANETs. *Electronics* **2022**, *11*, 2385. [CrossRef]
15. Shameem, A.; Singh, B.; Lourens, M.E. Intelligent Trust based e-learning based IDS system and VANET in 6G. *J. Pharm. Negat. Results* **2022**, *13*, 473–484. [CrossRef]
16. Zhou, H.; Xu, W.; Chen, J.; Wang, W. Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities. *Proc. IEEE* **2020**, *108*, 308–323. [CrossRef]
17. Jiang, H.; Xiong, B.; Zhang, H.; Basar, E. Hybrid Far- and Near-field Modeling for Reconfigurable Intelligent Surface Assisted V2V Channels: A Sub-Array Partition Based Approach. *IEEE Trans. Wirel. Commun.* **2023**, *22*, 8290–8303. [CrossRef]
18. Sharma, V.; You, I.; Guizani, N. Security of 5G-V2X: Technologies, Standardization, and Research Directions. *IEEE Netw.* **2020**, *34*, 306–314. [CrossRef]
19. Grover, J.; Prajapati, N.K.; Laxmi, V.; Gaur, M.S. Machine learning approach for multiple misbehavior detection in VANET. In *Advances in Computing and Communications, Proceedings of the First International Conference, ACC 2011, Kochi, India, 22–24 July 2011*; Proceedings, Part III 1; Springer: Berlin/Heidelberg, Germany, 2011; pp. 644–653.
20. Javed, F.; Khan, Z.A.; Rizwan, S.; Shahzadi, S.; Chaudhry, N.R.; Iqbal, M. A Novel Energy-Efficient Reservation System for Edge Computing in 6G Vehicular Ad Hoc Network. *Sensors* **2023**, *23*, 5817. [CrossRef]
21. Samara, G.; Al-Salihy, W.A.; Sures, R. Security issues and challenges of Vehicular Ad Hoc Networks (VANET). In Proceedings of the 4th International Conference on New Trends in Information Science and Service Science, Beijing, China, 30 June–20 July 2010; pp. 393–398.
22. Bian, K.; Zhang, G.; Song, L. Toward Secure Crowd Sensing in Vehicle-to-Everything Networks. *IEEE Netw.* **2018**, *32*, 126–131. [CrossRef]
23. Gopala, P.K.; Lai, L.; Gamal, H.E. On the Secrecy Capacity of Fading Channels. In Proceedings of the 2007 IEEE International Symposium on Information Theory, Toronto, ON, Canada, 6–11 July 2008.
24. Jameel, F.; Wyne, S.; Kaddoum, G.; Duong, T.Q. A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2734–2771. [CrossRef]
25. Dong, L.; Han, Z.; Petropulu, A.P.; Poor, H.V. Improving Wireless Physical Layer Security via Cooperating Relays. *IEEE Trans. Signal Process.* **2010**, *58*, 1875–1888. [CrossRef]
26. Wasef, A.; Lu, R.; Lin, X.; Shen, X. Complementing public key infrastructure to secure vehicular ad hoc networks [Security and Privacy in Emerging Wireless Networks]. *IEEE Wirel. Commun.* **2010**, *17*, 22–28. [CrossRef]
27. Epiphaniou, G.; Karadimas, P.; Kbaier Ben Ismail, D.; Al-Khateeb, H.; Dehghantanha, A.; Choo, K.R. Nonreciprocity Compensation Combined With Turbo Codes for Secret Key Generation in Vehicular Ad Hoc Social IoT Networks. *IEEE Internet Things J.* **2018**, *5*, 2496–2505. [CrossRef]
28. Karati, A.; Islam, S.H.; Biswas, G.P.; Bhuiyan, M.Z.A.; Vijayakumar, P.; Karuppiah, M. Provably Secure Identity-Based Signcryption Scheme for Crowdsourced Industrial Internet of Things Environments. *IEEE Internet Things J.* **2018**, *5*, 2904–2914. [CrossRef]
29. Tsai, J.L. A New Efficient Certificateless Short Signature Scheme Using Bilinear Pairings. *IEEE Syst. J.* **2017**, *11*, 2395–2402. [CrossRef]
30. Lai, C.; Zhou, H.; Cheng, N.; Shen, X.S. Secure Group Communications in Vehicular Networks: A Software-Defined Network-Enabled Architecture and Solution. *IEEE Veh. Technol. Mag.* **2017**, *12*, 40–49. [CrossRef]
31. Mathur, S.; Reznik, A.; Ye, C.; Mukherjee, R.; Rahman, A.; Shah, Y.; Trappe, W.; Mandayam, N. Exploiting the physical layer for enhanced security [Security and Privacy in Emerging Wireless Networks]. *IEEE Wirel. Commun.* **2010**, *17*, 63–70. [CrossRef]
32. Shiu, Y.S.; Chang, S.Y.; Wu, H.C.; Huang, S.C.H.; Chen, H.H. Physical layer security in wireless networks: A tutorial. *IEEE Wirel. Commun.* **2011**, *18*, 66–74. [CrossRef]
33. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Commun. Surv. Tutorials* **2014**, *16*, 1550–1573. [CrossRef]
34. Wang, C.; Wang, H.M.; Xia, X.G.; Liu, C. Uncoordinated Jammer Selection for Securing SIMOME Wiretap Channels: A Stochastic Geometry Approach. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 2596–2612. [CrossRef]
35. Wang, M.; Zhu, T.; Zhang, T.; Zhang, J.; Yu, S.; Zhou, W. Security and privacy in 6G networks: New areas and new challenges. *Digit. Commun. Netw.* **2020**, *6*, 281–291. [CrossRef]
36. Yang, N.; Shafie, A. Terahertz communications for massive connectivity and security in 6G and beyond era. *IEEE Communications Magazine*, 31 October 2022.
37. Abdelgader, A.M.; Shu, F. Exploiting the physical layer security for providing a simple user privacy security system for vehicular networks. In Proceedings of the 2017 International Conference on Communication, Control, Computing and Electronics Engineering (ICCCCEE), Khartoum, Sudan, 16–18 January 2017; pp. 1–6. [CrossRef]

38. Ghaderi, M.; Goeckel, D.; Orda, A.; Dehghan, M. Minimum Energy Routing and Jamming to Thwart Wireless Network Eavesdroppers. *IEEE Trans. Mob. Comput.* **2015**, *14*, 1433–1448. [CrossRef]
39. Yao, J.; Liu, Y. Secrecy Rate Maximization With Outage Constraint in Multihop Relaying Networks. *IEEE Commun. Lett.* **2018**, *22*, 304–307. [CrossRef]
40. Chen, G.; Coon, J.P.; Tajbakhsh, S.E. Secure Routing for Multihop Ad Hoc Networks With Inhomogeneous Eavesdropper Clusters. *IEEE Trans. Veh. Technol.* **2018**, *67*, 10660–10670. [CrossRef]
41. Shim, K.; Do, T.N.; An, B. A physical layer security-based routing protocol in mobile ad-hoc wireless networks. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Online, 11–14 February 2018; pp. 417–422. [CrossRef]