sensors

MDPI

Article

A Hybrid Price Auction-Based Secure Routing Protocol Using Advanced Speed and Cosine Similarity-Based Clustering against Sinkhole Attack in VANETs †

Yushintia Pramitarini [1], Ridho Hendra Yoga Perdana [1], Thong-Nhat Tran [2], Kyusung Shim [3] and Beongku An [3,*]

[1] Departement of Software and Communications Engineering in Graduate School, Hongik University, Sejong City 30016, Korea; yushintia@gmail.com (Y.P.); mail.rhyp@gmail.com (R.H.Y.P.)
[2] Departement of Electronics and Computer Engineering in Graduate School, Hongik University, Sejong City 30016, Korea; trantnhat@gmail.com
[3] Departement of Software and Communications Engineering, Hongik University, Sejong City 30016, Korea; shimkyusung@outlook.kr
* Correspondence:beongku@hongik.ac.kr

† This paper is an extended version of our paper published in Pramitarini, Y.; Tran, T.-N.; Shim, K.; Yulianto, A.W.; An, B. A Speed and Cosine Similarity-based Clustering for QoS Routing Protocol in Distributed Vehicular Ad-hoc Networks. In Proceedings of the 10th International Conference on Green and Human Information Technology (ICGHIT 2022), JeJu-si, Korea, 19–21 January 2022; pp. 109–113.

Abstract: In ad-hoc vehicle networks (VANETs), the random mobility causes the rapid network topology change, which leads to the challenge of the reliable data transmission. In this paper, we propose a hybrid-price auction-based secure routing (HPA-SR) protocol using advanced speed and cosine similarity-based (ASCS) clustering to establish a secure route to avoid sinkhole attacks and improve connectivity between nodes. The main features and contributions of the proposed HPA-SR protocol are as follows. First, the HPA-SR protocol is employed by the first- and second-price auctions to avoid sinkhole attacks. More specifically, using the Markov decision process (MDP), each node can select a kind of auction method to establish the secure route by avoiding the sinkhole attack. Second, the advanced speed cosine similarity clustering protocol that is considered as underlying structure is presented to improve the connectivity between nodes. The ASCS is constructed based on the cosine similarity and distance between nodes using the speed and direction of the nodes. The results of the performance show that the proposed HPA-SR protocol can establish the secure route avoiding the sinkhole attack while the proposed ASCS clustering can support the strong connectivity. Besides, the HPA-SR with ASCS protocol can show better performance than the benchmark protocol in terms of the routing delay, packet loss ratio, number of packet loss, and control overhead.

Keywords: secure routing; clustering; auction; security; sinkhole attack; vehicular ad-hoc networks

Citation: Pramitarini, Y.; Perdana, R.H.Y.; Tran, T.-N.; Shim, K.; An, B. A Hybrid Price Auction-Based Secure Routing Protocol Using Advanced Speed and Cosine Similarity-Based Clustering against Sinkhole Attack in VANETs. *Sensors* **2022**, *22*, 5811. https://doi.org/10.3390/s22155811

Academic Editor: Claudia Campolo

Received: 27 June 2022
Accepted: 30 July 2022
Published: 3 August 2022

1. Introduction

The development of hardware and wireless communication techniques can support communication between vehicles or vehicles and roadside units (RSU) [1,2]. However, since vehicles can dynamically and independently move, the direct transmission is very challenging. Thus, routing protocol is considered as one of the possible solutions to establish the route in vehicular ad-hoc networks (VANETs) [3–5]. In addition, the clustering protocols can enhance the stability of networks by making the clustering and electing the cluster head that can communicate with different cluster heads [6]. Thus, if the cluster exists in the network, the route connectivity is more stable than the network without clustering [7]. Since the centralized (managed) node does not exist in the VANETs, e.g., access point and base station, it is very vulnerable to the networking attacks. For example, denial of service (DOS) attack, blackhole attack, wormhole attack, sinkhole attack, etc. [8].

In VANETs, vehicles driving along roads can be formed into groups to facilitate communication. Clustering stabilizes the connectivity between nodes by hierarchizing the network architecture, where each cluster can be divided into three kinds of nodes, called cluster head (CH), cluster member (CM), and gateway (GW) [9,10]. When CM needs to communicate with other nodes, CM sends the message to its CH. This CH can communicate with other CHs. If the intermediate CH is out of transmission coverage, the GW helps to relay between CH and CH. When the data packet arrives at the last CH, the CH sends message to the desired CM.

Routing protocols play an essential role in ensuring reliable data communication [11]. The routing protocol can select the suitable next nodes from a source node to a destination node among intermediate nodes. Routing in a VANET is complicated due to its dynamic nature including significant mobility and various network topologies. Therefore, routing protocols designed for the VANET environment must meet the standards of scalability, efficiency, and comparability. Recently, the security has become one of the critical issues in the network [12]. Considering the accessibility of the network and also cyber security has drawn much attention for cyber-physical systems (CPS) [13]. Moreover, blockchain [14,15] is one of the solutions when it comes to supporting credible distributed communication, and basically having the main characteristics of decentralization, distributed consistency, etc. In VANET, there are three types of attacks. The first type is an attack on the communication infrastructure, such as routing protocols, the second type is an attack on VANET's functions, such as location monitoring, and the third type is an attack on security requirements, such as authentication protocols. The sinkhole attack is one of the network threats in which the sinkhole node announces itself as having the best path to the sink or destination node and prevents data transmission between a source and a destination node by broadcasting fake routing information [16,17]. During the routing process, the sinkhole node can provide fake information. Therefore, the data packet sent by the source node does not arrive at the destination node.

2. Related Work and Motivations

2.1. Related Works

Due to high mobility in VANETs, it brings the disconnection between nodes in urban scenarios. Therefore, we require a clustering protocol to achieve high stability as well as reducing control overhead. The author in [18] proposed a multi-hop broadcast protocol to efficiently disseminate emergency warning messages in a VANET with highway scenario. The authors in [19] proposed the lowest ID (LID) and highest degree (HD) algorithm. In the LID algorithm, the node with a lower identifier becomes a cluster head. In the HD algorithm, the node with the highest number of neighbors is selected as CH. The authors in [20] addressed the passive multi-hop clustering algorithm (PMC) to ensure the coverage and stability of the clusters. In [21], the authors studied the vehicle selection based on sigmoid function in which the vehicles with large object functions are selected as cluster heads. However, the proposed algorithm does not consider stability and connectivity between vehicles. Hence, to improve the network stability and connectivity, the network parameters that affect on the clustering and cluster head election is considered as the cost for clustering.

Various routing protocols have been proposed secure routing to tackle the node's strong mobility. The author in [22] addressed an intelligent opportunistic routing algorithm for wireless sensor networks and applies it for e-healthcare. The author in [23] presented an intelligent trust sensing scheme with metaheuristic-based secure routing protocol for Internet of Things in [23], to identify the next hope by using a fitness function. However, it cannot avoid the attacker directly in order to select the next hope. The author in [24] proposed a blockchain-based secure routing protocol for opportunistic networks. In [24], only registered nodes can forward hello packets. If there is a new node, the node must be registered first, then it can forward the hello packet. Otherwise, the node cannot join the network. The author in [25] studied a trust-based secure intelligent opportunistic

routing protocol to avoid the gray and black-hole attack in the wireless sensor networks. However, these works [22–25] proposed secure routing that did not focus on sinkhole attack in VANET. The authors in [26] addressed the method of speed adaptive beacon broadcast (SABB) to propagate information in urban and highway environments. In [27], the authors exploited the vulnerability attacks of distributed vehicular broadcast (DV-CAST) protocol and pointed out safety specifications that are necessary for DV-CAST security against specific attacks. Several studies had implemented sinkhole attack detection and prevention on networks. The authors in [28] proposed an individual trust managing (ITM) technique to prevent against sinkhole attack in MANETs. The authors in [29] presented an approach to prevent the sinkhole attack in mobile ad hoc networks (MANETs). In [29], hop count-based detection techniques is used to detect sinkhole attack. The proposed solution to detect the sinkhole node utilizes the non-propagating route request techniques. The authors in [30] proposed memory effective node collusion method to prevent and detect sinkhole and wormhole attacks using a modified AODV protocol. Su et al., in [31], studied the multi-path multi-hop routing in networks with selfish nodes. The authors in [32] proposed an algorithm based on auction mechanism for vehicle routing problem to ensure that the auction could be used in operational decision making. However, these secure routing protocol in [26–30] established the secure route against sinkhole attack without auction theory, which leads to the additional process to detect the sinkhole node. Different from [26–30], the work [31,32] proposed the auction theory-based secure routing protocols that did not require the sinkhole node detection process for the secure route establishment. Consequently, we can conclude that auction-based secure routing protocol can avoid the sinkhole attack without the detection process, which can reduce the control overhead and delay as well as sinkhole node avoiding. Therefore, the auction theory-based secure routing protocol is one of the possible solutions for VANETs.

2.2. Motivation and Contributions

Since the sinkhole attack causes various issues in VANETs, we propose the secure routing protocol to avoid the sinkhole attack. Different from the related works [19–21,26–32], in this paper, we propose a hybrid-price auction-based secure routing protocol (HPA-SR) to avoid the sinkhole attack without detection. The proposed secure routing protocol employs the Markov decision process (MDP) to select the next nodes as well as sinkhole node avoiding, where the MDP can switch from first price auction to second price auction based on the number of routes to avoid the sinkhole attack adaptively. In addition, we propose the mobility-based clustering protocol, called advanced speed and cosine similarity-based clustering (ASCS), to enhance the route stability and reduce the control overhead, which is modified by our previous work [33]. The proposed ASCS clustering protocol can enhance the route connectivity. The main contributions of this paper can be summarized as follows:

- We propose a novel hybrid price auction-based secure routing (HPA-SR) protocol to avoid sinkhole attacks. More specifically, the proposed HPA-SR protocol contains the first- and second-price auction. Each node employs the Markov decision process to conditionally select which kind of auction method used to establish the secure route against the sinkhole attack without detection.
- We further propose an advanced clustering protocol, called advanced speed and cosine similarity-based clustering (ASCS) protocol as underlying structure, to improve the route connectivity and reduce the control overhead in VANETs. The proposed clustering protocol consider node speed and direction as cosine similarity and cosine distance to form the clusters. In addition, the ASCS clustering protocol elects gateway nodes to support the communication between CHs when the next CHs is out of the transmission coverages.
- The performance evaluations show that the proposed routing protocol can establish more robust route against the sinkhole attack compared to that of AODV. Besides, the proposed ASCS clustering supports more strong connectivity since the clustering transforms the network topology hierarchically.

The rest of the paper is arranged as follows. Section 3 introduces the background theorem that consists of the background of auction theory, first-price auction, and second-price auction. Section 4 introduces the proposed routing protocol that consists of the basic concept of the proposed routing protocol, the proposed clustering protocol (ASCS) and the proposed hybrid-price auction-based secure routing protocol (HPA-SR). Section 5 presents the performance evaluation that consists of simulation environtments and parameters, performance metrics, and numerical results. Section 6 concludes the paper.

3. The Background Theorem: Auction Theory

3.1. The Background of Auction Theory

In this section, we present the process of establishing a secure route between a source and a destination node based on the auction theoretic algorithm. The auction theoretic algorithm belongs to a class of games in which a principal would like to condition the node's actions on some information that the other player privately knows. We design the hybrid-price auction-based secure routing (HPA-SR) protocol which consists of first- and second- price auction as explained in Section 4.4. Based on our auction model, the proposed HPA-SR protocol can avoid the sinkhole attack without detection and can also reduce the control overhead and delay while establishing a secure route.

In theory, the auction algorithm incorporates buying and selling items into the bid process [34]. In addition, the auction process is often used to sell objects that do not have a fixed or unspecified price. To simplify, we limit a single seller and only sell an item. Thus, the auction procedure can involve

- The seller offers only one item for sale,
- The i-th buyer of N buyers will have an object valuation (v_i) with $v_i \leq 0$.

3.1.1. First-Price Auction

The value of the player's bid affects whether or not the player wins and how much the player pays in the first-price auction. Thus, the most of the reasons for creating the previous section must be redone, and the conclusions have changed. We can suppose the auction is a game where players are bidders, and each bidder's strategy is the amount bid as a function of its true value. Suppose the winner of the game is player i, whose bid is b_i. Then, the payoff of player i is $v_i - b_i$ because the player i value for the sold object is v_i. For the other players the payoff is 0. It should be noted that the winner's payoff can be negative. This occurs when a player wins the object by overbidding or submitting a bid that is higher than her valuation of the object being sold. For two players participating in the auction, such as i and j, the payoff function of player p_i is [35]:

$$p_i = \begin{cases} v_i - b_i & b_i > b_j \\ 0 & b_i \leq b_j, \end{cases} \tag{1}$$

where i and j presents the two players in the auction, b_i is the bid of player i, and v_i is the value of the auction to player i. The theorem in [36] provides a thorough description of its Nash Equilibrium.

3.1.2. Second-Price Auctions

The winner of the second-price auction is the player who submitted the highest bid, but the player pays the seller the amount equal to the second highest bid [37]. If there are no ties in this auction, the winner pays a lower price to the seller than in the first-price auction, and the payoffs are now defined as follows:

$$p_i = v_i - \bar{b}, \tag{2}$$

where v_i always returns a non-negative payoff but can now produce a completely positive payoff and the highest bid $\bar{b} = \max b_j$, $j \neq i$. Note that if $v_i < b_i$ then there is still a winning

curse going on here and some other bids are in the open interval (v_i, b_i). There are Nash equilibrium of second-price auction:

- $(b_1, \cdots, b_n) = (v_1, \cdots, v_n)$, where each player's bid is equal to the other player's valuation.
- $(b_1, \cdots, b_n) = (v_1, 0, \cdots, 0)$, where player 1 gets the object and the other player's payoff is zero.

In these two equilibrium, we just described a player getting the object. However, there is a equilibria where the player does not get the object, such as $(b_1, \cdots, b_n) = (v_2, v_1, \cdots, 0)$, where another player gets an object with a price of v_2 and each player receives a zero payoff. We denote the second-price auction equilibrium is $(v_1, \cdots, v_n), (v_1, 0, \cdots, 0), (v_2, v_1, \cdots, v_n)$. However, the property suggests that this equilibrium is less plausible as an auction outcome than the first equilibrium, in which each player bids on the valuation of the other player. The last equilibrium's weakness is reflected in the fact that player 2's bid v_1 is weakly dominated by the bid v_2, as described in [38]. Besides that, it is very difficult to uncover the truth. However, in other cases, when a player bids less than another player, that player will never win. We need to show that when player i bids $b_i = v_i$, no deviation from this bid improves the other player's payoff, regardless of the strategy used by each player. There are two cases considered—the first case is when a deviation occurs in which i raises another player's bid, and the second case is when i lowers another player's bid.

The equilibrium of the second-price auction can be expressed as

$$(b_1, \cdots, b_n) = (v_1, \cdots, v_n) \tag{3}$$

where the bid of each player is equal to the valuation the player makes of the object. All other strategies of the player are weakly dominated by the player's action. Truthfulness is a dominant strategy that makes the second-price auction conceptually very clean. Regardless of what the other bidders do, the most honest bidder is the best choice. Then, the second-price auction will be used when the highest bidder is unfair, which makes sense when the highest bidder is overbidding or colluding. Thus, the second price auction can be expressed as

$$\max_{p_i} \; v_i - \bar{b} \neq 0, \tag{4}$$

where $\max_{p_i}$ is maximum payoff of the player i, then each player i has a value v_i, and the highest bid is $\bar{b}$. In other words, we determine that the maximum payoff of the player must not equal zero.

4. The Proposed Routing Protocol: HPA-SR

4.1. Basic Concept of the Proposed Routing Protocol

In this subsection, we present the basic concept of the proposed routing and clustering protocol. The proposed clustering (ASCS) protocol considers the speed and direction of the node to elect the cluster head while cosine similarity and cosine distance for forming the clusters (to decide the cluster members) are underlying structures to support stable connectivity between nodes.

The proposed routing protocol (HPA-SR) utilizes hybrid auction to establish the secure route from a source node to a destination node. As we can see in Figure 1, when the node receives various route information from the neighbor nodes, this node utilizes the second price auction to avoid the sinkhole attack. Therefore, the proposed HPA-SR protocol can establish the secure route such as S-CH_1-CH_3-$\cdots$-CH_k-D, which can avoid sinkhole node.

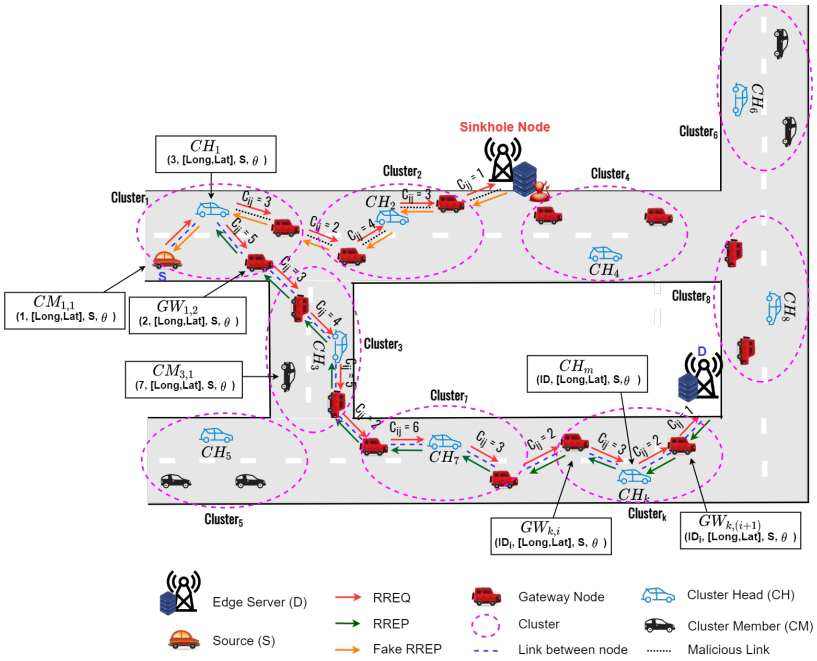


Figure 1. The basic concepts of the proposed routing protocol: HPA-SR.

The route establishment process consists of two steps which can be summarized as follows:

- **Step 1 (Clustering):** In the first step, we perform a clustering process in which all nodes in the network are divided into clusters by using cosine similarity method. We use the position, direction, and speed as parameters to make a cluster form that works as underlying structure. This work is a development of a paper that has been done by the author in [33]. The ASCS clustering protocol considers the gateway node to improve the route connectivity and reduce the control overhead.
- **Step 2 (Routing):** After the clustering step, using the hybrid auction method, a source node broadcasts the RREQ packet to find a destination node. When the intermediate nodes receive the RREQ packet, they update their routing table and re-broadcast the RREQ packet. When the RREQ packet arrives at the destination node, the destination unicasts the RREP packet. In addition, the sink hole node also unicasts the RREP packet. If the intermediate nodes receive the RREP packet from the different way, the node utilizes the second price auction to avoid the sinkhole attack. Otherwise, the intermediate nodes employ the first-price auction.

4.2. The Proposed Clustering Protocol (ASCS): The Underlying Structure

4.2.1. The Basic Concepts of the ASCS

As shown in Figure 2, the proposed clustering protocol [33], called advanced speed and cosine similarity-based clustering (ASCS) protocol as underlying structure, can improve the route connectivity and reduce the control overhead in VANETs. The proposed clustering protocol consider node speed and direction as cosine similarity and cosine distance to form the clusters. In addition, the ASCS clustering protocol elects gateway nodes to support the communication between CHs when the next CHs is out of the transmission coverages. Figure 3 demonstrates the flowchart of the proposed ASCS clustering protocol. The proposed ASCS clustering protocol consists of two sub-subsections, which can be summarized in the following subsection.

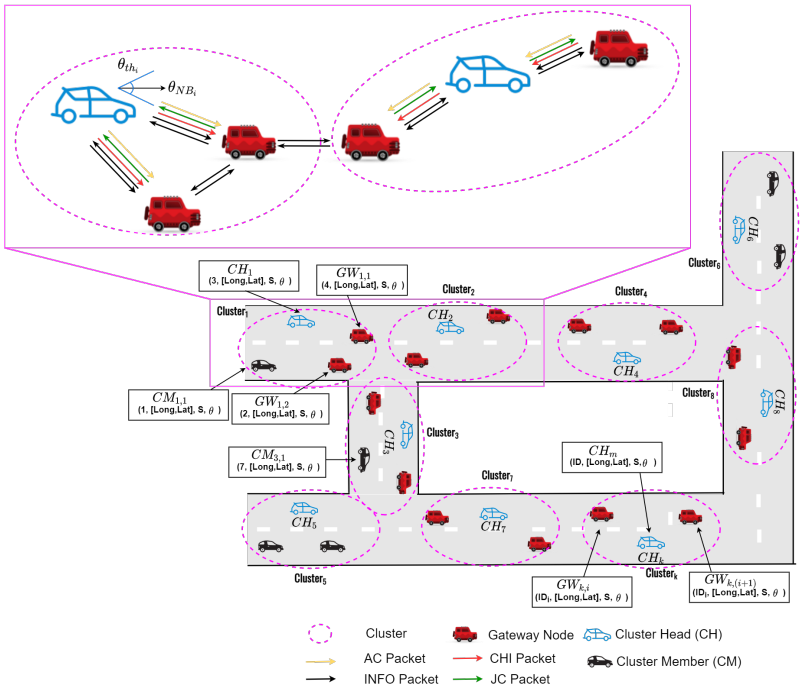


Figure 2. The basic concepts of the ASCS clustering protocol.

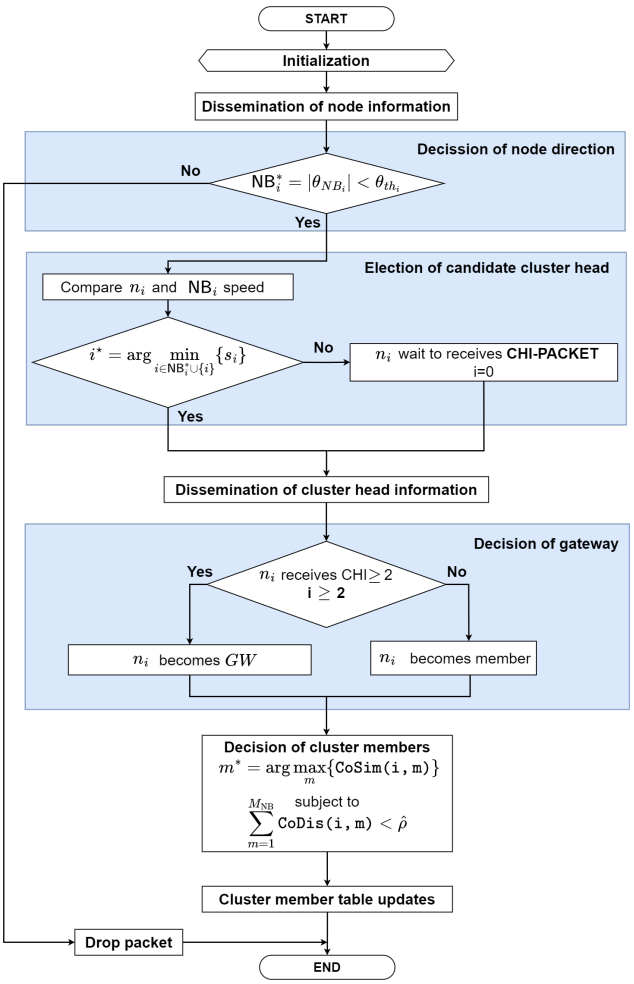


Figure 3. The flowchart of the proposed clustering protocol: ASCS.

4.2.2. The Proposed Clustering Protocol: ASCS

In this sub-subsection, we explain in detail the proposed clustering protocol, named ASCS. We consider two criteria to form the cluster, namely cosine similarity and cosine distance. The procedure for electing the cluster head and forming a cluster (to decide the cluster members) is as follows:

- **Step 0: Initialization**
  When the clustering starts, each node turns on and operates independently.
- **Step 1: Dissemination of Node Information**
  A node n_i estimates its information, such as speed, direction, and location, periodically. To advertise its node information with neighbor nodes, node n_i generates **(INFO)** packet and broadcasts the **(INFO)** packet to its neighbor nodes periodically, respectively. **INFO** packet contains the following fields:

$$\langle \texttt{Type}, \texttt{S}_{\texttt{ID}}, \texttt{D}_{\texttt{ID}}, \texttt{S}, \texttt{Dir} \rangle$$

  where `Type` represents packet type, $\texttt{S}_{\texttt{ID}}$ represents source node ID, $\texttt{D}_{\texttt{ID}}$ represents destination node ID, `S` represents i-th node's speed, and `Dir` represents its node direction (θ_i), respectively.
- **Step 2: Decission of Node Direction**
  When n_i receives **INFO** packet from the neighbor nodes as shown in Figure 2, the n_i checks whether the direction is less than the threshold of the neighbor nodes and if it will be cluster head (CH) or not, which is mathematically expressed as

$$\mathsf{NB}_i^* = |\theta_{NB_i}| < \theta_{th_i}, \tag{5}$$

  where θ_{NB_i} is direction nodes and θ_{th_i} is threshold direction of i-th node. The selected nodes means that they can move in the same direction.
  - If $\mathsf{NB}_i = \mathsf{NB}_i^*$, go to **step 3**.
  - Otherwise, the packet will be dropped.
- **Step 3: Election of Candidate Cluster Heads**
  The candidate cluster heads (CHs) are selected by the slowest node among the two or more neighbor nodes, which is mathematically expressed as

$$i^\star = \arg \min_{i \in \mathsf{NB}_i^* \cup \{i\}} \{s_i\}. \tag{6}$$

  Since the cluster head is the smallest node speed in the similar direction, this node can provide strong connectivity between the cluster head and the cluster member nodes.
  - If $i = i^\star$, the node n_i becomes cluster head, go to **step 4**.
  - Otherwise, go to **step 6**.
- **Step 4: Dissemination of Cluster Head Information**
  If n_i becomes the cluster head, to announce to its neighbor nodes, n_i generates and broadcasts the cluster head information **(CHI)** packet to its neighbor nodes. The **CHI** packet contains the following fields:

$$\langle \texttt{Type}, \texttt{S}_{\texttt{ID}}, \texttt{D}_{\texttt{ID}}, \texttt{S}, \texttt{Loc}, \texttt{Dir} \rangle$$

  where `Type` represents packet type, $\texttt{S}_{\texttt{ID}}$ represents source node ID, $\texttt{D}_{\texttt{ID}}$ represents destination node ID, `S` represents its node speed, `Loc` represents its node location (x_i, y_i), `Dir` represents its node direction (θ_i), respectively. Then, go to **step 7**.
- **Step 5: Decision of Gateway**
  When n_i is between more than one cluster heads, n_i will receive more than one **CHI** packet from cluster heads neighbor. Next, n_i becomes the gateway node. Otherwise, n_i becomes member node, and go to **step 6**.

- **Step 6: Decision of Cluster Members**
  Node n_i decides the cluster head among the candidates of the cluster head using link stability based on Cosine Similarity and Cosine Distance, as follows. The cosine similarity and cosine distance are used to calculate the link stability between n_i and neighbor nodes. The selected cluster member (CM_{m^*}) can be mathematically formulated as:

$$m^\star = \arg\max_{m} \{\mathtt{CoSim(i,m)}\}, m \in \mathsf{CH}_{\mathsf{NB}_i}, \tag{7a}$$

$$s.t. \quad \sum_{m=1}^{M_{\mathsf{NB}}} \mathtt{CoDis(i,m)} < \hat{\rho}, \tag{7b}$$

  where $\mathsf{CH}_{\mathsf{NB}_i}$ represents a set of cluster heads near n_i, M_{NB} represents the number of CMs near node i, i.e., $M_{\mathsf{NB}} = |\mathrm{CM}_{NB_m}|$. (7a) indicates the maximum cosine similarity between n_i and CH_m, while (7b) means the cosine distance constraint that must be less than the cosine distance threshold ($\hat{\rho}$). In (7b), $\mathtt{CoSim}$ can be expressed as [39].

$$\mathtt{CoSim(i,m)} = \frac{\sum_{m=1}^{N} \overrightarrow{V}_i \overrightarrow{V}_m}{\sqrt{\sum_{i=1}^{N} \overrightarrow{V}_i^2} \sqrt{\sum_{m=1, m\neq i}^{N} \overrightarrow{V}_m^2}}, \tag{8}$$

  where $\overrightarrow{V}_i$ and $\overrightarrow{V}_m$ are the i-th and m-th node's vector information, respectively. Each node $\overrightarrow{V}_i$ is related with a mobility vector information metric value (i.e. speed, direction, and location) $\overrightarrow{V}_i = (\overrightarrow{V}_1, \overrightarrow{V}_2, \cdots, \overrightarrow{V}_m)$, where $\overrightarrow{V}_i$ constitutes the vector values which indicate link information between nodes. Cosine similarity can determine the similarity information from each adjacent node, while cosine distance is a method for determining the communication distance between adjacent node. By considering the maximum cosine similarity under the constrained communication distance, we can control the cluster member to make more stable cluster members in the viewpoint of mobility. Then, the cosine distance of the node used to find the distance between two nodes can be calculated by [40]

$$\mathtt{CoDis(i,m)} = \{1 - \mathtt{CoSim(i,m)}\}. \tag{9}$$

  If n_i selects the CH_{m^*}, the node CH_{m^*} can be as the best cluster head. Node n_i sends the joint-cluster **(JC)** packet to the CH_{m^*}. **JC** packet contains the following fields:

$$\langle \mathtt{Type}, \mathtt{S_{ID}}, \mathtt{D_{ID}}, \mathtt{S}, \mathtt{Loc}, \mathtt{Dir}, \mathtt{Status} \rangle$$

  where $\mathtt{Type}$ represents packet type, $\mathtt{S_{ID}}$ represents source node ID, $\mathtt{D_{ID}}$ represents destination node ID, $\mathtt{S}$ represents its node speed (s_i), $\mathtt{Loc}$ represents its node location (x_i, y_i), $\mathtt{Dir}$ represents its node direction, and $\mathtt{Status}$ represents its node status (gateway node or else), respectively. Then, go to **step 7**.
- **Step 7: Cluster Member Table Updates**
  Node n_i replies the accept **(AC)** packet to the transmitted node and updates the cluster member (CM) table and the cluster has been formed. **AC** packet contains the following fields:

$$\langle \mathtt{Type}, \mathtt{S_{ID}}, \mathtt{D_{ID}}, \mathtt{Status} \rangle$$

  where $\mathtt{Type}$ represents packet type, $\mathtt{S_{ID}}$ represents source node ID, $\mathtt{D_{ID}}$ represents destination node ID, and $\mathtt{Status}$ represents its node status (gateway node or else), respectively.
  - Otherwise, n_i waits until it receives **AC** packet.

It is noted that, according to the characteristic of vehicular networks, the nodes dynamically and randomly move. Thus, the members often switch from one cluster to another cluster. However, the member nodes (including the source node and gateway node) do not switch much through the proposed clustering algorithm. The possible reason is that the cluster has a similar mobility pattern via cosine similarity and cosine distance. Besides, since the cluster head is the slowest node, the cluster head does not switch much. Table 1 is summarized the list of packets for the proposed clustering protocol process.

Table 1. List of Packets for The ASCS clustering protocol.

Packet Name	Full Name	Field Information
INFO	Information Packet	$\texttt{Type}, \texttt{S}_{\texttt{ID}}, \texttt{D}_{\texttt{ID}}, \texttt{S}, \texttt{Dir}$
CHI	Cluster Head Info Packet	$\texttt{Type}, \texttt{S}_{\texttt{ID}}, \texttt{D}_{\texttt{ID}}, \texttt{S}, \texttt{Loc}, \texttt{Dir}$
JC	Joint-Cluster Packet	$\texttt{Type}, \texttt{S}_{\texttt{ID}}, \texttt{D}_{\texttt{ID}}, \texttt{S}, \texttt{Loc}, \texttt{Dir}, \texttt{Status}$
AC	Accept-Cluster Packet	$\texttt{Type}, \texttt{S}_{\texttt{ID}}, \texttt{D}_{\texttt{ID}}, \texttt{Status}$

4.3. The Proposed Hybrid-Price Auction-Based Secure Routing Protocol: HPA-SR

In this subsection, we explain in detail the proposed hybrid-price auction-based secure routing protocol, named HPA-SR protocol. As can be observed in Figure 4, the source node S begins to establish a routing route to the destination node D.

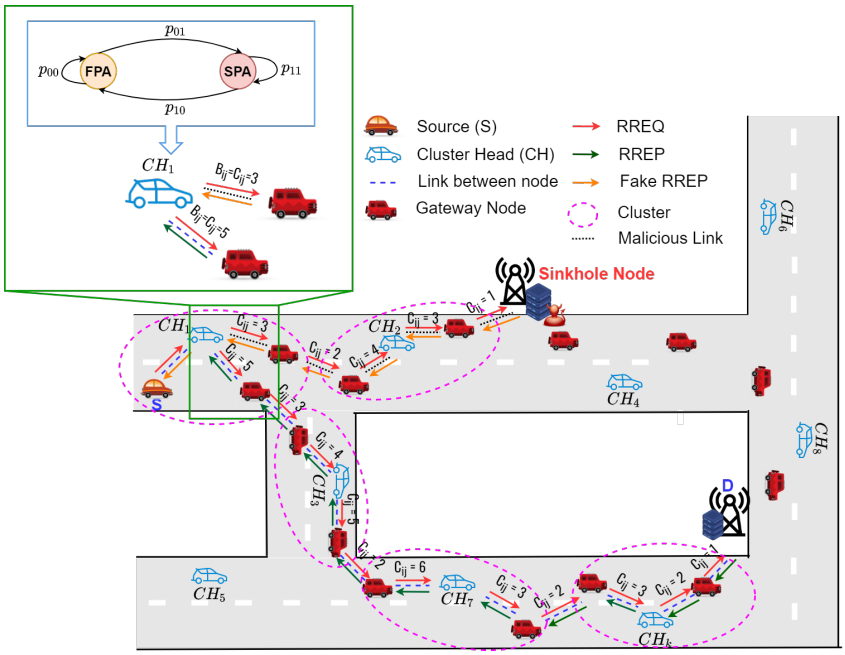


Figure 4. The proposed routing protocol: HPA-SR.

The event of route establishment happens (on demand-reactive). We propose a HPA-SR protocol that contains the first price auction (FPA) and second price auction (SPA) in which each node employs the Markov decision process (MDP) to select which kind of auction method is used to establish the secure route by avoiding the sinkhole attack, as explained in Section 4.4. Figure 5 illustrates the flowchart of the proposed routing procedure, which can be summarized as follows:

Route Request Process:

- **Step 1: Initialization**
  The source node S starts to establish a routing route between the source node S and the destination node D.

- **Step 2: Source Node Operation for Route Request: Generates and Sends RREQ Packet**
If the source node S does not have the routing information to the destination node D, the source node S generates a RREQ packet and sends RREQ packet to the cluster head CH_k in its cluster. The RREQ packet contains the following fields:

$$\langle \mathsf{Type}, \mathsf{S_{ID}}, \mathsf{D_{ID}}, \mathsf{S_{Seq}}, \mathsf{D_{Seq}}, \mathsf{RREQ_{ID}}, \mathsf{hop} \rangle$$

where Type represents packet type, $\mathsf{S_{Seq}}$ is the source sequence, and $\mathsf{D_{Seq}}$ is the destination sequence, which is the number of attempts to confirm control messages, $\mathsf{RREQ_{ID}}$ is the number of generating RREQ packet on the same session at the source, and hop is denoted as the number of hop to the destination, respectively.
- **Step 3: Intermediate Node Operation at Cluster Head for Route Request**
When CH_k receives the RREQ packet, CH_k records sender's ID and updates the routing table, then CH_k broadcasts RREQ to the gateway node ($\mathsf{GW_k}$) in its cluster or the next cluster heads and goes to **step 4**.
- **Step 4: Intermediate Node Operation at Gateway for Route Request**
When the gateway node $\mathsf{GW_k}$ receives RREQ packet from CH_k, $\mathsf{GW_k}$ records sender's ID and updates the routing table, then $\mathsf{GW_k}$ broadcasts RREQ to their neighbors node NB_k and goes to **step 5**. Otherwise, RREQ packet will be dropped.

Route Reply Process:

- **Step 5: Destination Node Operation for Route Reply: Generates and Sends RREP Packet**
When NB_k is the destination node D, the destination node D records sender's ID and updates the routing table, then generates a RREP packet. The destination node D unicasts the RREP packet to the previous node. The RREP packet contains the following fields:

$$\langle \mathsf{Type}, \mathsf{S_{ID}}, \mathsf{D_{ID}}, \mathsf{Energy}, \mathsf{D_{Seq}}, \mathsf{hop} \rangle$$

where Energy represents remaining energy of the node. Then, go to **step 6**
- **Step 6: Intermediate Node Operation at Previous Node (to the source node) for Route Reply**
When the intermediate node NB_j receives RREP packet, NB_j records sender's ID of RREP packet and updates the routing table. Then, go to **step 7**. Otherwise, NB_j waits until it receives RREP packet.
- **Step 7: Calculation of Cost/Bidding Value for Secure Route Establishment**
The intermediate node NB_j calculates cost/bidding value b_j. NB_j will compare the cost/bidding value b_j receiving with the bidding threshold B_{th}. If the b_i is greater than B_{th}, NB_j will use second price auction (SPA) to determine the route to be pursued by the next node. Otherwise, if the b_i is less than B_{th}, then NB_j will use first price auction (FPA) to determine the route to be traversed by the next node. NB_j will select the next node for data transmission based on a hybrid price auction process model that adaptively decides the auction model among the first price auction and the second price auction against the sinkhole attack, then we will obtain the routing table that can be summarized in Table 2, where PN is previous node, NB_j as next node NN , Cost is cost/bidding value, $\mathsf{S_{ID}}$ is source ID and $\mathsf{D_{ID}}$ is destination ID, respectively. The routing table will be used to determine the next node to the destination node that will be passed by the data packet during the data transmission process. Besides, we will explain the detailed process of hybrid price auction in Section 4.4. Then, go to data transmission process in **step 8**.

Data Transmission Process:

- **Step 8: Data Transmission at Source Node**
The source S sends data packet to the destination D based on the routing table, which is determined in **Step 1** to **Step 7**.

Table 2. Routing table of the proposed HPA-SR protocol.

PN	NN	Cost	S_{ID}	D_{ID}

The list of packet for the HPA-SR protocol can be summarized in Table 3.

Table 3. List of packets for the HPA-SR protocol.

Packet Name	Full Name	Field Information
RREQ	Route request	Type, S_{ID}, D_{ID}, S_{Seq}, D_{Seq}, $RREQ_{ID}$, hop
RREP	Route reply	Type, S_{ID}, D_{ID}, Energy, D_{Seq}, hop

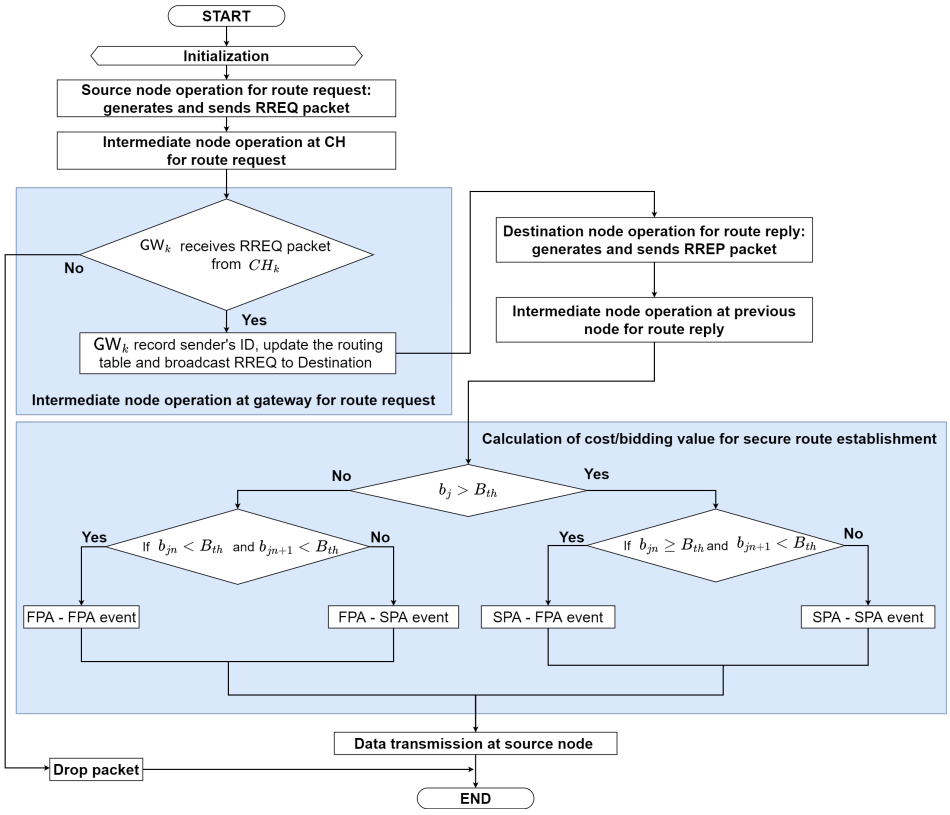


Figure 5. The flowchart of the proposed routing protocol: HPA-SR.

4.4. The Hybrid-Price Auction Model Process for The Proposed HPA-SR Protocol

As we can see in Figure 4, a sinkhole attack occurs when a node tries to attack the data of a trusted neighbor by broadcasting fake routing information and then proceeding to the destination node. A sinkhole attack has behavior in choosing the best route in the network. We can solve this problem by using a hybrid-price auction in secure routing to avoid sinkhole attacks. In other words, the source will choose the best route using first or second-price auction to send data transmission to the destination. In this paper, we consider the secure routing protocol based on hybrid-price auction. Therefore, we present the hybrid-price auction model process for the proposed the routing protocol, HPA-SR. In this analysis, we will drive to select the kind of auction model. In secure routing protocol, the sets of players are included as the intermediate nodes and denoted as $N = 1, 2, \cdots, n$. Thus, the valuation of each nodes is $v_1 > v_2 > \cdots > v_n > 0$. The node valuations of the object are assumed to be all different and all positive. We assume that each intermediate node receives a per-packet cost for forwarding packets and that this cost is private to itself. Each node i bids b_i its outbound link cost, which is reported during the route discovery

process, and each node i can only bid one time. We use (3) as the equilibrium of hybrid-price auction. In summary, the hybrid-price auction is the following strategic game:

Players: The set $I = 1, 2, \cdots, i$ of the n bidders. In this case, players are the intermediate nodes.
Action: Action is what the player will do. In this case, each player will make a bid.
Payoff: Since $b_i < B_{th}$, the players play the first-price auction. Otherwise, players play the second-price auction. If $b_i \geq B_{th}$, we denote $\bar{b}$ as the highest submitted by a player other i as in (4).

- If $b_i \leq \bar{b}$, the number of each other player who bids $\bar{b}$ is greater than b_i, then the maximum payoff of the i-th player is $v_i - \bar{b}$ where $\max_{p_i}$ is not equal to zero.

We aim to design an hybrid-price auction that consists of the first-price auction (FPA) and second-price auction (SPA) model to help for determining the route to be chosen by the next node. Based on [35,37] for either FPA or SPA strategies, let b_i denote the bidding value of the node, S_n represents the session of the network. In this work, the basic concept of the hybrid-price auction can be modeled as a two-state Markov chain with the FPA and SPA states, respectively, as illustrated in Figure 4. In state FPA, the node will use FPA to determine the route to be pursued by the next node, and in state SPA, the node will use SPA to determine the route to be traversed by the next node. The transition of the FPA/SPA strategies can be explained as follows. For illustration, suppose that each node receives an RREP packet from the previous node. We consider remaining energy to get the cost/bidding value because sinkhole nodes and edge servers have unlimited energy while intermediate nodes have limited energy. Thus, we combine the number of hops and the remaining energy of each node to obtain the cost/bidding value. The cost/bidding value is calculated by multiplying the number of hops by the remaining energy of each node, which is expressed as:

$$b_i = \mathsf{hop}_i \times ER_i, \tag{10}$$

where hop_i represents the number of hops of node i and ER_i represents remaining energy of node i as explained in Section 4.5. Then, the node will compare the cost/bidding value that is received with the cost/bidding threshold. There are two scenarios to compare the cost/bidding value with the cost/bidding threshold. If b_i is less than B_{th}, the node will use FPA to determine the route to be pursued by the next node. Otherwise, if b_i is greater than B_{th}, the node will use SPA to determine the route to be traversed by the next node. Accordingly, there are four transition events between the two states as follows:

Event 1: The FPA-FPA event: $S_n + S_{n+1}$, $b_{in} < B_{th}$ and $b_{in+1} < B_{th}$,
Event 2: The FPA-SPA event: $S_n + S_{n+1}$, $b_{in} < B_{th}$ and $b_{in+1} \geq B_{th}$,
Event 3: The SPA-FPA event: $S_n + S_{n+1}$, $b_{in} \geq B_{th}$ and $b_{in+1} < B_{th}$,
Event 4: The SPA-SPA event: $S_n + S_{n+1}$, $b_{in} \geq B_{th}$ and $b_{in+1} \geq B_{th}$,

Where S_n represents the n-th session, S_{n+1} represents the next session, b_{in} represents the cost/bidding on node i in session n, and b_{in+1} represents bidding on node i in the next session, respectively. From the transition events, it is noteworthy that: when $b_{in} < B_{th}$, the node will choose the route with the first auction price and when $b_{in} \geq B_{th}$, the node will choose the route with the second auction price, regardless of the conditions on each session. For steady-state probabilities, let p_{00}, p_{01}, p_{10}, and p_{11} denote the transition probabilities of events one to four, respectively. Let π_1 and π_0 denote the steady-state probabilities of the FPA and SPA status, respectively. The relationship between π_1 and π_0 associated with the described Markov chain can be expressed as [41]

$$\begin{aligned} \pi_0 &= p_{00}\pi_0 + p_{10}\pi_1, \\ \pi_1 &= p_{01}\pi_0 + p_{11}\pi_1, \\ 1 &= \pi_0 + \pi_1. \end{aligned} \tag{11}$$

Relying on the fact that $p_{00} = 1 - p_{01}$ and $p_{11} = 1 - p_{10}$, and after some modifications, π_0 and π_1 can be written as

$$\pi_0 = \frac{p_{10}}{1 - p_{00} + p_{10}} = \frac{p_{10}}{p_{01} + p_{10}}, \tag{12}$$

$$\pi_1 = \frac{p_{01}}{1 - p_{11} + p_{01}} = \frac{p_{01}}{p_{01} + p_{10}}. \tag{13}$$

4.5. Energy Consumption Model

In this paper, we used an energy model to calculate the energy consumption for sending and receiving packet over a link [42,43]. As we can see in Figure 6, the energy model will be used for the HPA-SR to calculate the residual energy required by the sender and receiver to send a number of packets. Therefore, a node can choose the next node to send data so that the residual energy of the sender and receiver is greater than the energy threshold, thereby extending the life of the route. We consider that all nodes are equipped with IEEE 802.11a 11 Mbps network interface card, whose electric currents are 280 mA and 330 mA in reception mode and transmission mode, respectively, and the electric potential is 5 V [44]. The remaining energy ER_i at node i-th can be formulated as:

$$ER_i = ER_{pi} - E_{\text{mode}} \quad [\text{joule}], \tag{14}$$

where ER_{pi} is the current remaining energy of the node i-th, and E_{mode} is energy consumption model that has transmit or receive modes. The energy consumption model when node i-th transmits and receives data packet p is expressed mathematically as follows.

$$\mathsf{E}_{\mathsf{Tx}}(\mathsf{i}, \mathsf{p}) = \mathrm{I}_{\mathrm{tx}} \times V \times t_{\mathsf{p}} \quad [\text{joule}], \tag{15}$$

$$\mathsf{E}_{\mathsf{Rx}}(\mathsf{i}, \mathsf{p}) = \mathrm{I}_{\mathrm{rx}} \times V \times t_{\mathsf{p}} \quad [\text{joule}] \tag{16}$$

where I_{tx} and I_{rx} represent the electric currents of transmission and reception, respectively. V is the electric potential, and t_{p} represents the time taken to transmit the packet p (in seconds).

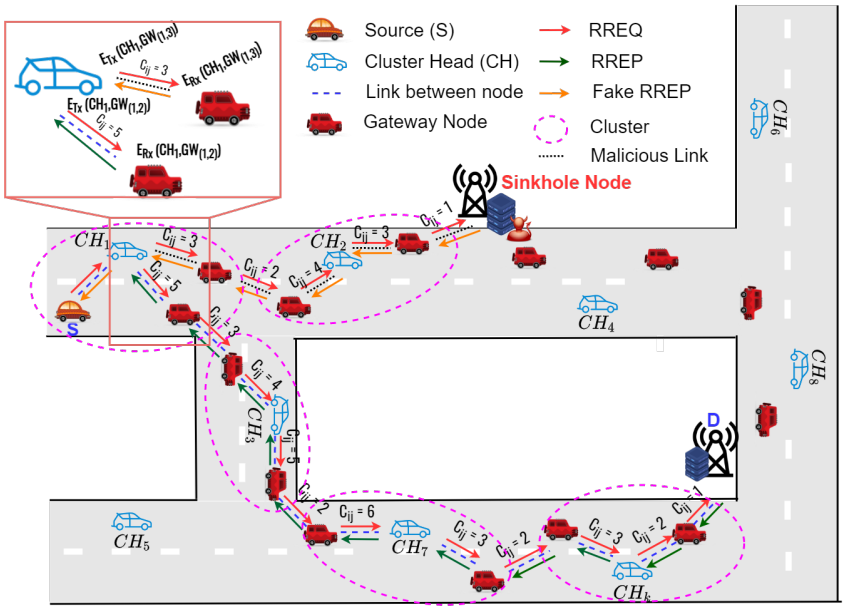


Figure 6. The basic concepts of the energy consumption model for the HPA-SR.

5. Performance Evaluation

5.1. Simulation Environments and Parameters

In the simulation, to provide more insight into the proposed routing protocol and clustering, we compared the performance of the HPA-SR protocol with AODV routing protocol. The simulation environments and parameters are presented in Table 4. In particular, we deployed 30, 50, and 100 nodes moving over an area of size 1000 × 1000 m^2 in urban scenario. In this case, mobile nodes move according to the group mobility. The nodes are divided into groups, and several groups will move in the same direction. The groups will build their movements based on the group leader's movement [45]. The initial position of nodes is randomly distributed along the street and moves with different speeds (20 km/h, 40 km/h, 60 km/h, and 80 km/h) [46]. The MAC layer is modeled using the IEEE 802.11 standard, and using the received signal strength indicator (RSSI) threshold is −80 dBm for communication range to more practically. One of the reasons for considering the use of RSSI is that the value of fluctuations in RSSI obtained has taken into account its effect on changes in channel conditions including multi-path fading [47]. All the simulation experiments are carried out on the NS3 simulator.

Table 4. Simulation Environments and Parameters.

Parameters	Value
Simulator	NS3
Simulation area	1000 × 1000 m^2
Packet size	1024 bits
Mobility model	Group Mobility
Radio range	250 m
Simulation time	200 s
Session length	5 s
Number of nodes	[30, 50, 100]
Node's Speed Range	[20:20:80] (km/h)
Receive signal strength indicator (RSSI) threshold	−80 dBm
MAC protocol	802.11a

5.2. Performance Metrics

The performances of the proposed routing and the clustering protocols, HPA-SR and ASCS, are evaluated in terms of the following metrics:

- Packet delivery ratio (PDR): it is defined by the ratio of the number of the received data packet at the destination node over the number of the transmitted data packet at the source node.
- Delay: it is defined by the average latency to establish the route per one session.
- Control overhead: it is defined by the average number of control packets to establish a route per session per node.
- The average number of the cluster head change: it is defined by the average number of cluster heads changes in per cluster per session [33].
- Packet loss ratio: it is defined by the ratio of the number of packets loss to the total number of sent packets [48].

5.3. Numerical Results

In this subsection, we present illustrative simulation results for the achievable performance of the proposed HPA-SR protocol approach. In particular, we set in the simulations parameter as shown in Table 4. We use the NS3 simulation program, where the algorithm is run with 200 s with 5 s each sessions. The simulation results in every figure are obtained with an average of 40 independent session.

To illustrate the effectiveness of suggested algorithm (HPA-SR with ASCS), we will compare the performance of the suggested algorithm with AODV protocol (with or without combining ASCS clutering protocol).

Figure 7 represents the comparison of the average number of cluster head changes in each session as a function of node speed to evaluate cluster stability. As can be seen in Figure 7, when the node speed increases, the average number of cluster head change is increased. One of possible reasons is that when the node speed is increased, the node location is changed frequently, which causes the broken of clustering. In addition, when the number of node in the network increases, the average number of cluster head change is increased. It can be explained as when the density of networks increase, the cluster head is changed. Nevertheless, the average number of cluster head change is less than one. It means that the number of cluster head change is less than one in each session. Thus, the proposed clustering is very stable.

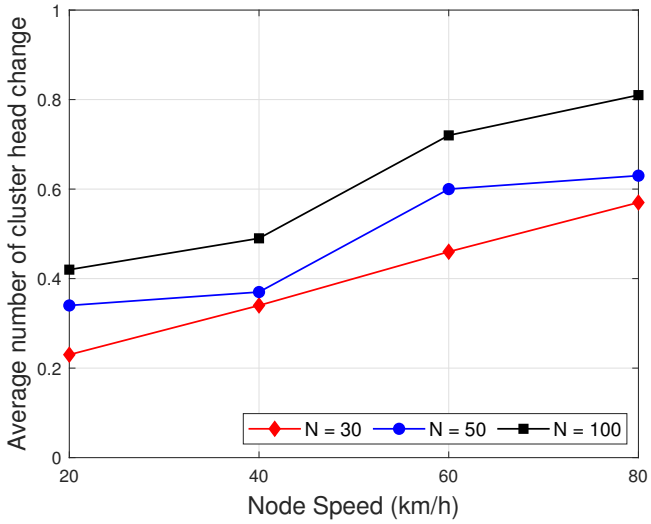


Figure 7. Average number of the cluster head change as a function of node speed.

Figure 8 shows the comparison of the packet delivery ratio as a function of node speed. As can be seen in Figure 8, when the node speed increases, the packet delivery ratio is decreased. One of the possible reasons is that when the node speed is increased, the entire network becomes more unstable and dynamic as velocity reaches higher values, which causes packet loss. However, we can notice that the decrease in packet delivery ratio is significantly less in the case of HPA-SR with ASCS (HPA-SR+ASCS) protocol than in other cases. Thus, HPA-SR with ASCS protocol proved to be the most reliable in terms of packet delivery ratio.

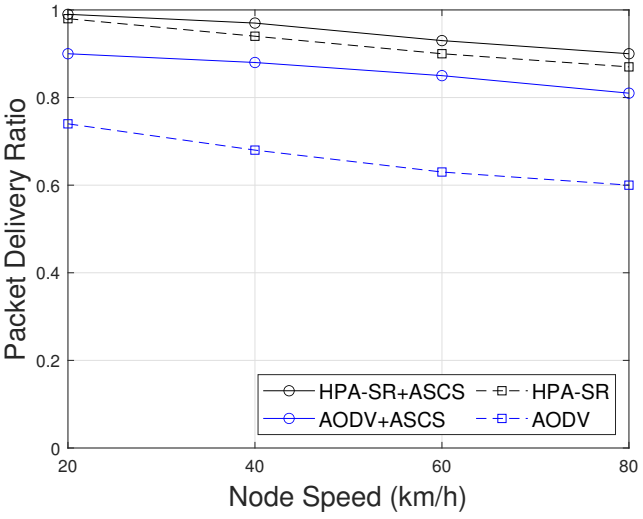


Figure 8. PDR as a function of node speed with difference scenarios.

Figure 9 presents the comparison of the routing delay including latency time for cluster construction per session as a function of node speed. As can be seen in Figure 9, the pattern of routing delay is shown to increase when the node speed increases. This result can be explained as the route establishment spending more time because the node moves more dynamically. However, the proposed HPA-SR with ASCS (HPA-SR+ASCS) protocol only involves the CH and GW nodes to determine the route to be traversed by the packet. Thus, the HPA-SR+ASCS protocol can send packets with a minimum delay compared to other protocols.

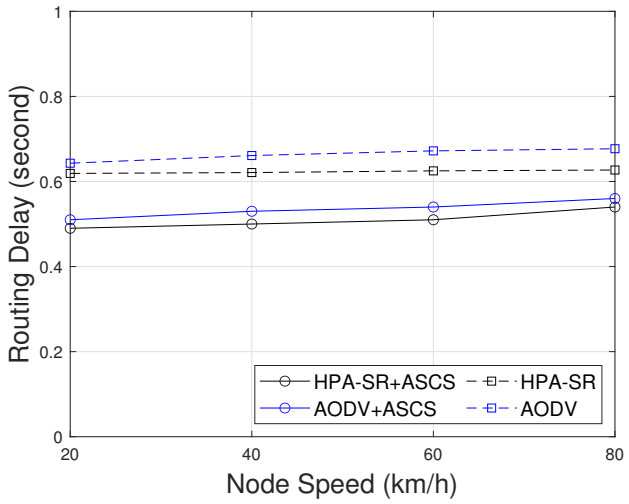


Figure 9. Routing delay as a function of node speed with different scenarios.

Figure 10 represents the comparison of the control overhead including the control overhead for cluster construction per node per session as a function of node speed. As shown in Figure 10, when the speed increases, the control overhead is increased little bits, but not significant. One of the possible reasons is that if node speed increases, the distance is increased, which causes the need for more packets to establish the route. However, ASCS clustering protocol can reduce the control overhead in our proposed routing protocol compared with other cases. It means that ASCS clustering protocol only involves CH and GW in the routing process and the decrease in control overhead is significantly less in case HPA-SR+ASCS protocol than in other cases. Thus, the HPA+ASCS protocol demonstrated that it can improve connectivity while also being the most stable in terms of control overhead.

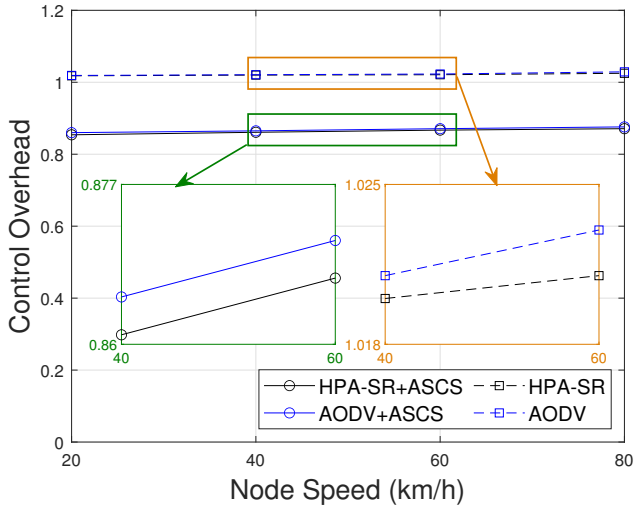
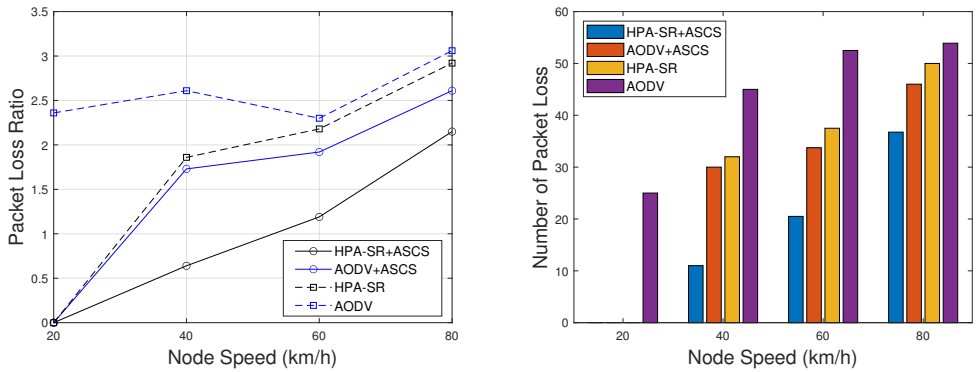


Figure 10. Control overhead as function of node speed with difference scenarios.

Now, we turn to our attention to security perspective. Figure 11 shows the comparison of the average packet loss ratio Figure 11a and number of packet loss Figure 11b in each session as a function of node speed in km/h, respectively. The average packet loss ratio shown in Figure 11a is defined by the ratio of the number of loss packets to the total number of sent packets. As can observed in Figure 11a, when the node speed increases, the average packet loss ratio is increased. At the same time in Figure 11b, when the node speed increases, the average number of packet loss is increased. One of the possible reasons is that when the node speed increase, the location is changed frequently, which causes the packet to be sent directly to the sinkhole node. However, we can notice that the clustering can reduce the number of links between nodes. Thus, the proposed HPA-SR+ASCS protocol is proved to be secure in terms of network security perspective.



(**a**) Packet loss ratio vs node speed (**b**) Number of packet loss vs node speed

Figure 11. The comparison of packet loss ratio and number of packet loss as a function of node speed with different scenarios.

Finally, we exploit the impact of the number of nodes on the network metrics. In Figure 12, we evaluate the packet delivery ratio in the effect of the number of node on the proposed routing protocol with the proposed clustering as a function of node speed with a different number of nodes. As we can see in Figure 12, when the node speed is increased, the PDR will decrease a little bit. Besides, when the number of node increases, the PDR will be increased little bit. The reason is that when the number of node increases, the density of network is increased, which provides more strong connectivity between nodes. The HPA-SR+ASCS protocol with number of nodes N = 100 outperforms with the high packet delivery ratio.

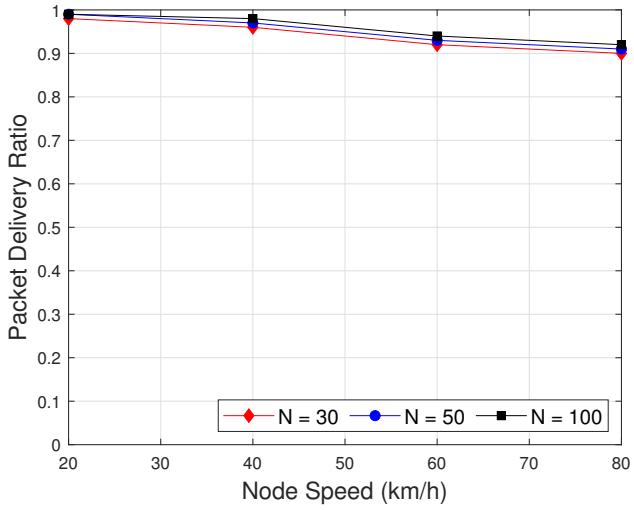


Figure 12. Packet delivery ratio as function of node speed with different number of nodes.

Figure 13 presents the routing delay in the effect of the number of node on the proposed routing protocol with the proposed clustering as a function of node speed with different number of nodes. As can be seen in Figure 13, when the node speed and the number of node increases, the routing delay is increased little bits, but not significantly. It can be explained that when the number of node and speed increased, the number of hop is increased, which causes the routing process to take longer.

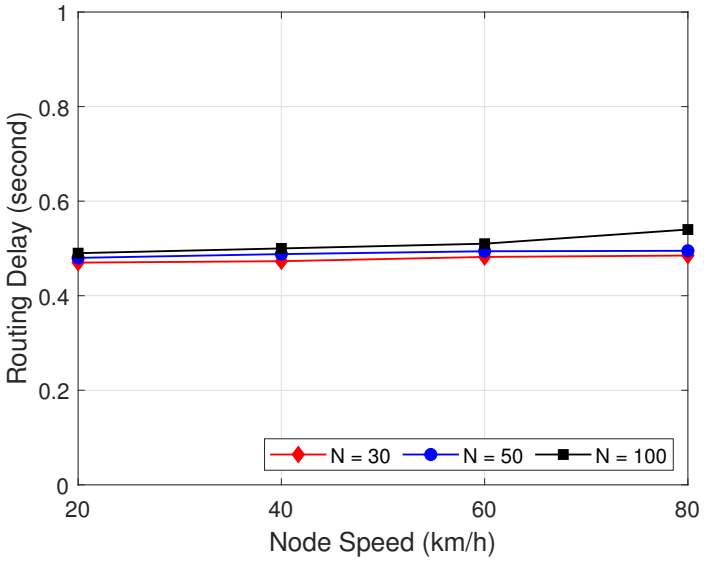


Figure 13. Routing delay as a function of node speed with different number of nodes.

Figure 14 presents the control overhead as function of node speed with different number of nodes on HPA-SR+ASCS protocol with different number of nodes. As can be observed in Figure 14, when the speed and number of nodes increases, the control overhead is increased. There are two possible reasons as follows. Firstly, when the number of node increases, the density of the network is increased, which leads to the increasing of RREQ and RREP packet transmission frequency. Secondly, when the number of node speed increases, since the node is more easily broken, the control overhead is increased.

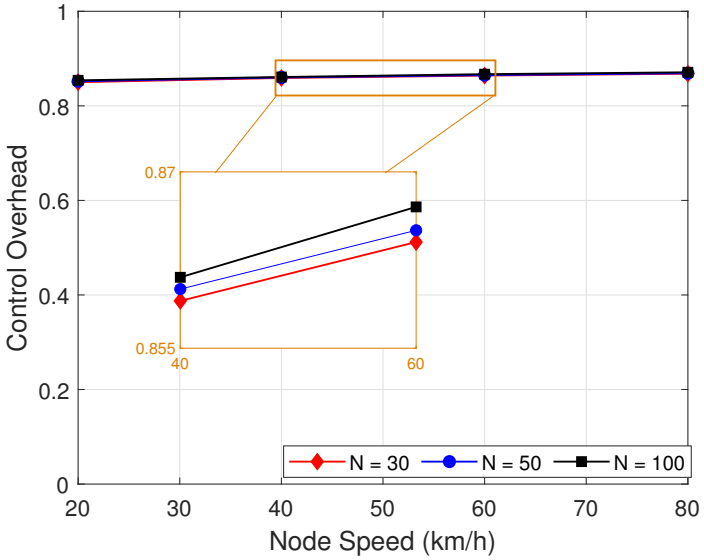


Figure 14. Control overhead as function of node speed with different number of nodes.

6. Conclusions

In this paper, we proposed a hybrid-price auction-based secure routing (HPA-SR) protocol and an advanced speed and cosine similarity-based clustering (ASCS) protocol as an underlying structure to establish a secure route against sinkhole attacks and improve connectivity between nodes. The proposed HPA-SR protocol used the first- and second-price auction to avoid sinkhole attacks. Each node was used in the Markov decision process to conditionally select which kind of auction method establishes the secure route against the sinkhole attack. Besides, to improve connectivity between nodes, the proposed ASCS clustering protocol that works as underlying structure used the node's speed and direction and then calculated the cosine similarity and distance between nodes. The numerical results showed that the use of hybrid-price auction and advanced speed cosine similarity improves the performance of routing in the network. The proposed HPA-SR with ASCS outperforms either the AODV+ASCS, HPA-SR, or AODV protocol in terms of the security in the network and packet delivery ratio. Additionally, the proposed HPA-SR with ACSS protocol are able to reduce the routing delay, packet loss ratio, number of packet loss, and control overhead.

Author Contributions: Y.P.: Conceptualization, Validation, Writing—original draft. R.H.Y.P.: Conceptualization, Validation, Writing—review and editing. T.-N.T.: Conceptualization, Validation, Writing—review and editing. K.S.: Conceptualization, Validation, Writing—review and editing. B.A.: Conceptualization, Funding acquisition, Project administration, Writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NRF-2022R1A2B5B01001190). Beongku An is the corresponding author.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Ullah, A.; Yao, X.; Shaheen, S.; Ning, H. Advances in Position Based Routing towards ITS Enabled FoG-Oriented VANET-A Survey. *IEEE Trans. Intell. Transp. Syst.* **2020**, *21*, 828–840. [CrossRef]
2. Lin, D.; Kang, J.; Squicciarini, A.; Wu, Y.; Gurung, S.; Tonguz, O. MoZo: A Moving Zone Based Routing Protocol Using Pure V2V Communication in VANETs. *IEEE Trans. Mob. Comput.* **2017**, *16*, 1357–1370. [CrossRef]
3. Hui, Y.; Cheng, N.; Su, Z.; Huang, Y.; Zhao, P.; Luan, T.H.; Li, C. Secure and Personalized Edge Computing Services in 6G Heterogeneous Vehicular Networks. *IEEE Internet Things J.* **2021**, *4662*, 1–12. [CrossRef]
4. Al-Sultan, S.; Al-Doori, M.M.; Al-Bayatti, A.H.; Zedan, H. A Comprehensive Survey on Vehicular Ad Hoc Network. *J. Netw. Comput. Appl.* **2014**, *37*, 380–392. [CrossRef]
5. Khilar, P.; Bhoi, S. Vehicular communication: A survey. *IET Netw.* **2014**, *3*, 204–217.
6. Pramitarini, Y.; Tran, T.N.; An, B. Energy Consumption Location-Based QoS Routing Protocol for Vehicular Ad-Hoc Networks. In Proceedings of the 2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 20–22 October 2021; pp. 1266–1270.
7. Alsarhan, A.; Al-Dubai, A.Y.; Min, G.; Zomaya, A.Y.; Bsoul, M. A New Spectrum Management Scheme for Road Safety in Smart Cities. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 3496–3506. [CrossRef]
8. Samvatsar, M. Security Improvement of Mobile Ad Hoc Networks using Clustering Approach. *Int. J. Comput. Sci. Inf. Technol.* **2016**, *7*, 1638–1642.
9. Wang, H.; Liu, R.P.; Ni, W.; Chen, W.; Collings, I.B. VANET Modeling and Clustering Design Under Practical Traffic, Channel and Mobility Conditions. *IEEE Trans. Commun.* **2015**, *63*, 870–881. [CrossRef]
10. Ozera, K.; Bylykbashi, K.; Liu, Y.; Barolli, L. A security-aware fuzzy-based cluster head selection system for VANETs. In *Innovative Mobile and Internet Services in Ubiquitous Computing, Proceedings of the International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Matsue, Japan, 4–6 July 2018*; Springer: Cham, Switzerland, 2018; Volume 773, pp. 505–516.
11. Joahannes, J.B.; de Souza, A.M.; Rosário, D.; Cerqueira, E.; Villas, L.A. Efficient data dissemination protocol based on complex networks' metrics for urban vehicular networks. *J. Internet Serv. Appl.* **2019**, *10*, 15.

12. Kaur, R.; Scholar, M.; Pal, T.; Singh, M.; Khajuria, V.; Scholar, M. Security Issues in Vehicular Ad-Hoc Network(VANET). In Proceedings of the 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 11–12 May 2018; pp. 884–889.
13. Sedjelmaci, H.; Guenab, F.; Senouci, S.M.; Moustafa, H.; Liu, J.; Han, S. BLCS: Brain-Like Distributed Control Security in Cyber Physical Systems. *IEEE Netw.* **2020**, *34*, 6–7. [CrossRef]
14. Yang, H.; Liang, Y.; Yuan, J.; Yao, Q.; Yu, A.; Zhang, J. Distributed Blockchain-Based Trusted Multidomain Collaboration for Mobile Edge Computing in 5G and beyond. *IEEE Trans. Ind. Inform.* **2020**, *16*, 7094–7104. [CrossRef]
15. Yang, H.; Bao, B.; Li, C.; Yao, Q.; Yu, A.; Zhang, J.; Ji, Y. Blockchain-Enabled Tripartite Anonymous Identification Trusted Service Provisioning in Industrial IoT. *IEEE Internet Things J.* **2022**, *9*, 2419–2431. [CrossRef]
16. Liu, Y.; Ma, M.; Liu, X.; Xiong, N.N.; Liu, A.; Zhu, Y. Design and Analysis of Probing Route to Defense Sink-Hole Attacks for Internet of Things Security. *IEEE Trans. Netw. Sci. Eng.* **2020**, *7*, 356–372. [CrossRef]
17. Muzammal, S.M.; Murugesan, R.K.; Jhanjhi, N.Z. A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust-Based Approaches. *IEEE Internet Things J.* **2021**, *8*, 4186–4210. [CrossRef]
18. Javed, M.A.; Ngo, D.T.; Khan, J.Y. A multi-hop broadcast protocol design for emergency warning notification in highway VANETs. *Eurasip J. Wirel. Commun. Netw.* **2014**, *2014*, 1–15. [CrossRef]
19. Gavalas, D.; Pantziou, G.; Konstantopoulos, C.; Mamalis, B. Lowest-ID with Adaptive ID Reassignment: A Novel Mobile Ad-Hoc Networks Clustering Algorithm. In Proceedings of the 2006 1st International Symposium on Wireless Pervasive Computing, Phuket, Thailand, 16–18 January 2006; pp. 1–5.
20. Zhang, D.; Ge, H.; Zhang, T.; Cui, Y.Y.; Liu, X.; Mao, G. New Multi-Hop Clustering Algorithm for. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 1517–1530. [CrossRef]
21. Ge, X.; Gao, Q.; Quan, X. A novel clustering algorithm based on mobility for VANET. 2018 IEEE 18th International Conference on Communication Technology (ICCT), Chongqing, China, 8–11 October 2018; pp. 473–477.
22. Bangotra, D.K.; Singh, Y.; Selwal, A.; Kumar, N.; Singh, P.K.; Hong, W.C. An Intelligent Opportunistic Routing Algorithm for Wireless Sensor Networks and Its Application Towards e-Healthcare. *Sensors* **2020**, *20*, 3887. [CrossRef] [PubMed]
23. Gali, S.; Nidumolu, V. An intelligent trust sensing scheme with metaheuristic based secure routing protocol for Internet of Things. *Cluster Comput.* **2022**, *25*, 1779–1789. [CrossRef]
24. Dhurandher, S.K.; Singh, J.; Nicopolitidis, P.; Kumar, R.; Gupta, G. A blockchain-based secure routing protocol for opportunistic networks. *J. Ambient Intell. Humaniz. Comput.* **2022**, *13*, 2191–2203. [CrossRef]
25. Bangotra, D.K.; Singh, Y.; Selwal, A.; Kumar, N.; Singh, P.K. A Trust Based Secure Intelligent Opportunistic Routing Protocol for Wireless Sensor Networks. *Wirel. Pers. Commun.* **2021**. [CrossRef]
26. Kad, S.; Banga, V.K. An Optimized Speed Adaptive Beacon Broadcast Approach for Information Dissemination in Vehicular Ad hoc Networks. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 2850–2860.
27. Almasri, A.; Chaddoud, G. Security of the Distributed Vehicular Broadcast Protocol DV-CAST. *Int. J. Comput. Appl.* **2020**, *177*, 26–31. [CrossRef]
28. Jebadurai, I.J.R.; Rajsingh, E.B.; Paulraj, G.J.L. Enhanced dynamic source routing protocol for detection and prevention of sinkhole attack in mobile ad hoc networks. *Int. J. Netw. Sci.* **2016**, *1*, 63. [CrossRef]
29. Agrwal, S.L.; Khandelwal, R.; Sharma, P.; Gupta, S.K. Analysis of detection algorithm of Sinkhole attack & QoS on AODV for MANET. In Proceedings of the 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 14–16 October 2016; pp. 839–842.
30. Sasirekha, D.; Radha, N. Secure and Attack Aware Routing in Mobile AdHoc Networks against Wormhole and Sinkhole Attacks. In Proceedings of the 2017 2nd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 19–20 October 2017; pp. 505–510.
31. Su, X.; Chan, S.; Peng, G. Auction in Multi-Path Multi-Hop Routing. *IEEE Commun. Lett.* **2009**, *13*, 154–156.
32. Karels, V.C.; Veelenturf, L.P.; Van Woensel, T. An auction for collaborative vehicle routing: Models and algorithms. *EURO J. Transp. Logist.* **2020**, *9*, 100009. [CrossRef]
33. Pramitarini, Y.; Tran, T.n.; Shim, K.; Yulianto, A.W.; An, B. A Speed and Cosine Similarity-based Clustering for QoS Routing Protocol in Distributed Vehicular Ad-hoc Networks. In Proceedings of the 10th International Conference on Green and Human Information Technology, JeJu, Korea, 19–21 January 2022; pp. 109–113.
34. Easley, D.; Kleinberg, J. Auctions. In *Networks, Crowds, Mark. Reason. About a Highly connected World*; Cambridge University Press: Cambridge, UK, 2010; Chapter 9, pp. 249–273.
35. Zhang, W.; Wang, X.; Han, G.; Peng, Y.; Guizani, M. SFPAG-R: A Reliable Routing Algorithm Based on Sealed First-Price Auction Games for Industrial Internet of Things Networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 5016–5027. [CrossRef]
36. Bergemann, D.; Brooks, B.; Morris, S. First-Price Auctions With General Information Structures: Implications for Bidding and Revenue. *Econometrica* **2017**, *85*, 107–143. [CrossRef]
37. Vickrey, W.S. Counterspeculation, Auctions, And Competitive Sealed Tenders. *J. Financ.* **1961**, *16*, 8–37. [CrossRef]
38. Hershberger, J.; Suri, S. Vickrey Pricing in Network Routing: Fast Payment Computation. In Proceedings of the 42nd Annual Symposium on Foundations of Computer Science, Las Vegas, NV, USA, 14–17 October 2001; pp. 252–259.
39. Nahar, A.; Sikarwar, H.; Das, D. CSBR: A Cosine Similarity Based Selective Broadcast Routing Protocol for Vehicular Ad-Hoc Networks. In Proceedings of the 2020 IFIP Networking Conference (Networking), Paris, France, 22–26 June 2020; pp. 404–412.

40. Abosamra, G.; Oqaibi, H. Using Residual Networks and Cosine Distance-Based K-NN Algorithm to Recognize On-Line Signatures. *IEEE Access* **2021**, *9*, 54962–54977. [CrossRef]
41. Do, T.N.; Da Costa, D.B.; Duong, T.Q.; An, B. Improving the Performance of Cell-Edge Users in MISO-NOMA Systems Using TAS and SWIPT-Based Cooperative Transmissions. *IEEE Trans. Green Commun. Netw.* **2018**, *2*, 49–62. [CrossRef]
42. De Rango, F.; Guerriero, F.; Fazio, P. Link-Stability and Energy Aware Routing Protocol in Distributed Wireless Networks. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 713–726. [CrossRef]
43. Shan, A.; Fan, X.; Wu, C.; Zhang, X.; Fan, S. Quantitative Study on the Impact of Energy Consumption Based Dynamic Selfishness in MANETs. *Sensors* **2021**, *21*, 716. [CrossRef]
44. Feeney, L.M.; Nilsson, M. Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment. In Proceedings of the IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No.01CH37213), Anchorage, AK, USA, 22–26 April 2001; Volume 3, pp. 1548–1557.
45. Al-Qassas, R.S. Routing and the Impact of Group Mobility Model in VANETs. *J. Comput. Sci.* **2016**, *12*, 223–231. [CrossRef]
46. Amina, B.; Mohamed, E. Performance Evaluation of VANETs Routing Protocols Using SUMO and NS3. In Proceedings of the 2018 IEEE 5th International Congress on Information Science and Technology (CiSt), Marrakech, Morocco, 21–27 October 2018; pp. 525–530.
47. Shrestha, S.; Laitinen, E.; Talvitie, J.; Lohan, E.S. RSSI channel effects in cellular and WLAN positioning. In Proceedings of the 2012 9th Workshop on Positioning, Navigation and Communication, Dresden, Germany, 15–16 March 2012; pp. 187–192.
48. Sirajuddin, M.; Rupa, C.; Iwendi, C.; Biamba, C. TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network. *Secur. Commun. Netw.* **2021**, *2021*, 5521713. [CrossRef]