






## Article

# Toward Blockchain-Enabled Privacy-Preserving Data Transmission in Cluster-Based Vehicular Networks

Gyanendra Prasad Joshi <sup>1</sup>, Eswaran Perumal <sup>2</sup>, K. Shankar <sup>2</sup>, Usman Tariq <sup>3,\*</sup>,  
Tariq Ahmad <sup>3</sup> and Atef Ibrahim <sup>3</sup>

<sup>1</sup> Department of Computer Science and Engineering, Sejong University, Seoul 05006, Korea; joshi@sejong.ac.kr

<sup>2</sup> Department of Computer Applications, Alagappa University, Karaikudi, Tamil Nadu 630003, India; eswaran@alagappauniversity.ac.in (E.P.); drkshankar@ieee.org (K.S.)

<sup>3</sup> College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia; t.hanger@psau.edu.sa (T.A.); aa.mohamed@psau.edu.sa (A.I.)

\* Correspondence: u.tariq@psau.edu.sa; Tel.: +966-5071-96057

Received: 22 July 2020; Accepted: 18 August 2020; Published: 21 August 2020



**Abstract:** In recent times, vehicular ad hoc networks (VANET) have become a core part of intelligent transportation systems (ITSs), which aim to achieve continual Internet connectivity among vehicles on the road. The VANET has been used to improve driving safety and construct an ITS in modern cities. However, owing to the wireless characteristics, the message transmitted through the network can be observed, altered, or forged. Since driving safety is a major part of VANET, the security and privacy of these messages must be preserved. Therefore, this paper introduces an efficient privacy-preserving data transmission architecture that makes use of blockchain technology in cluster-based VANET. The cluster-based VANET architecture is used to achieve load balancing and minimize overhead in the network, where the clustering process is performed using the rainfall optimization algorithm (ROA). The ROA-based clustering with blockchain-based data transmission, called a ROAC-B technique, initially clusters the vehicles, and communication takes place via blockchain technology. A sequence of experiments was conducted to ensure the superiority of the ROAC-B technique, and several aspects of the results were considered. The simulation outcome showed that the ROAC-B technique is superior to other techniques in terms of packet delivery ratio (PDR), end to end (ETE) delay, throughput, and cluster size.

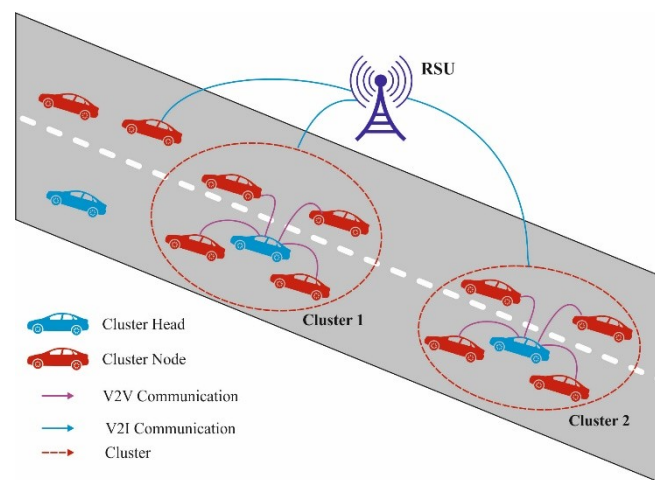
**Keywords:** blockchain; clustering; privacy; inter-vehicle communication vehicular networks; security; rainfall optimization algorithm

## 1. Introduction

Vehicular ad hoc networks (VANET) have been developed as a subset of a mobile ad hoc network (MANET) [1]. MANET is a method for smart transportation modules, like intelligent transportation systems (ITSs). Many developers have begun using the VANET in the wireless mobile communication sector. A major feature of VANET is that it offers inter-vehicle communication and roadside units to enhance road security, local traffic flow, and effectiveness of road traffic by offering precise and periodic data for road users [2]. VANET offers two kinds of communications: vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). On-board units (OBUs) and roadside units (RSUs) in a VANET deploy correlations using dedicated short-range communication (DSRC).

The load balancing of a VANET has to be maintained for while the network is improved. Here smart clustering models are very important, and are used for developing a vehicular network with a remarkably efficient, adaptable, reliable, and equalized load distribution. Clustering in a system means that nodes are collected according to their merits and demerits to attain better network

performance. In a group or cluster, a single cluster member (CM) has been elected as the cluster head (CH). In a VANET, vehicles are used as network nodes and are grouped into clusters, as shown in Figure 1. This can be classified as an NP-hard problem. CH election is central to the clustering approach. The CH carries out various operations, like cluster deployment, termination of a cluster, and maintenance of resources, and assumes the network topology for provisioning. The CH also has to manage communication among clusters, both internal and external, with other accessible clusters in the system.



**Figure 1.** General cluster-based Vehicular ad hoc networks (VANET) architecture. RSU: roadside units.

A VANET provides different functionalities and resources, especially driver security, infotainment, and directional guidance [3]. The VANET prioritizes safety over non-safety information. Safety data warns the drivers in case of any threat, and provides a solution. However, VANET also has some problems, mostly with security and privacy while transmitting data [4]. Whenever the vehicles enter or exit highways, they have to follow safety measures, determined by factors like traffic congestion, road conditions, roadwork, and many others. These factors should be considered when making decisions to reach the destination without interruption. These details must be updated regularly to avoid delays. In particular, the malicious nodes may ignore or intentionally change the essential safety details before sending the information to the user, which may lead to tragic consequences. In addition, the features of VANET, like mobility and volatility, are variable, and wireless communication networks have vulnerable to VANETs in massive internal and external attacks [5].

Because of the decentralized structure and the dynamic topology of VANETs, the safety of vehicles, users, and information is important, and malicious nodes should be identified [6]. In a VANET, vehicles exchange confidential data, and traffic is modified accordingly. The absence of authorized data leads to malevolent attacks that cause serious problems for the drivers [7]. The messages can be authorized by tracking the vehicles through a network and finding the details required [8]; however, this compromises the security of users. Therefore, a balance should be found between authentication and the privacy of users. Trust management and privacy of vehicles are challenging problems for VANETs.

A blockchain has been developed, and it is distributed, along with the decentralized common database of transactions, using electronic operations at participating nodes [9]. The blockchain is effective because of features such as decentralization, anonymity, the chronological sequence of data, shared security, transparency, immutability, and suitability for unsecured platforms [10]. It is assumed that the platform is secure while the aggregated processing energy of malicious nodes is not effective compared to the processing energy of trusted nodes [11]. In the study of VANETs, earlier works have found that secure event message dissemination depends on voting [12]. Many of the voting models try to resolve the problems of node security by using alternate nodes for computing the trustworthiness of a node. Hence, these models face challenges regardless of whether the feedback provided by nodes is

authentic or not. In our work, by contrast, every detail is placed in a distributed database using the blockchain approach.

As the driving safety is a major aim of VANETs, it is important to protect the security and privacy of these messages. We have developed an efficient privacy-preserving data transmission architecture that makes use of the blockchain model for ensuring privacy in cluster-based VANETs. The vehicles in the VANET are clustered using a rainfall optimization algorithm (ROA), which groups the vehicles into several clusters, and a CH is chosen for every cluster. This results in effective load balancing and minimum overhead in the network. The ROA-based clustering with blockchain-based data transmission is called a ROAC-B technique. It initially clusters the vehicles, and communication takes place via blockchain technology.

We ran a set of simulation processes to verify the effectiveness of the ROAC-B technique, and considered several aspects of the results.

The remaining sections of the paper are arranged as follows. Section two briefly outlines a few works relevant to the study. Section three discusses the proposed ROAC-B technique, and Section four validates the technique. Finally, Section five concludes the paper.

## 2. Related Works

Different types of security models have been presented by different researchers to analyze the security issues of VANETs. The authentication scheme smart card (ASC) was developed to report the security-conservation issues like the legitimacy of users and data being forwarded by a system [13]. The authorization of users and messages is performed through low-cost cryptographic tasks. This method does not validate the user's identity, or the authenticity of the details that are conveyed. Wazid et al. [14] proposed a decentralized lightweight authentication and key agreement protocol (LAKAP) for VANETs, which uses one-way hash functions and bitwise exclusive OR (XOR) operations. Rajput et al. [15] developed a hybrid method for a privacy-preserving authentication approach (HEPPA) that combines the characteristics of pseudonym-reliant models and cluster signature-dependent methods, along with conditional anonymity.

Tangade and Manvi [16] proposed an effective, scalable, and privacy-preserving authentication (ESPA) protocol with the help of a hybrid cryptography scheme for intervehicle communications. ESPA contains two phases: V2I pre-authentication and V2V authentication. Cui et al. [17] presented a secure privacy-preserving authentication scheme for VANETs in conjunction with a cuckoo filter (SPACF) to improve the security and privacy of users and to reduce the communication burden.

Limited work has been performed on vehicular networks that use blockchain. Lei et al. [18] used a fundamental blockchain for simplifying distributed key observation in assorted vehicular networks. Leiding et al. [19] integrated the VANET with Ethereum's blockchain-dependent application, and activated a visible, self-monitoring, and decentralized module. It uses Ethereum's smart contract method for implementing an Ethereum blockchain. Dorri et al. [20] presented a blockchain concept for automotive security using overlay networks in the blockchain, as well as additional nodes called overlay block managers. The deployment of extra overlay nodes leads to a large delay, which is a center point of failure. Rowan et al. [21] introduced a blockchain for securing communication of smart vehicles using visible light communication and acoustic side channels. The blockchain is used with public keys for the validation of the proposed model using cryptographic session keys, by using side channels, as well as a blockchain public key structure.

Inspired from the software-defined and function virtualization abilities of edge-cloud interplay, Song et al. [22] introduced an effective smart collaborative tracking model by the use of advanced parameter prediction skills and enhanced particle filtering techniques. Initially, the range-based positioning problems are converted into the vector nonlinear suboptimal approximation problem depending upon information fusion. Next, the significance of the density function is provided for calculating the location and trajectory of the mobile nodes by attaining cubature points, update state

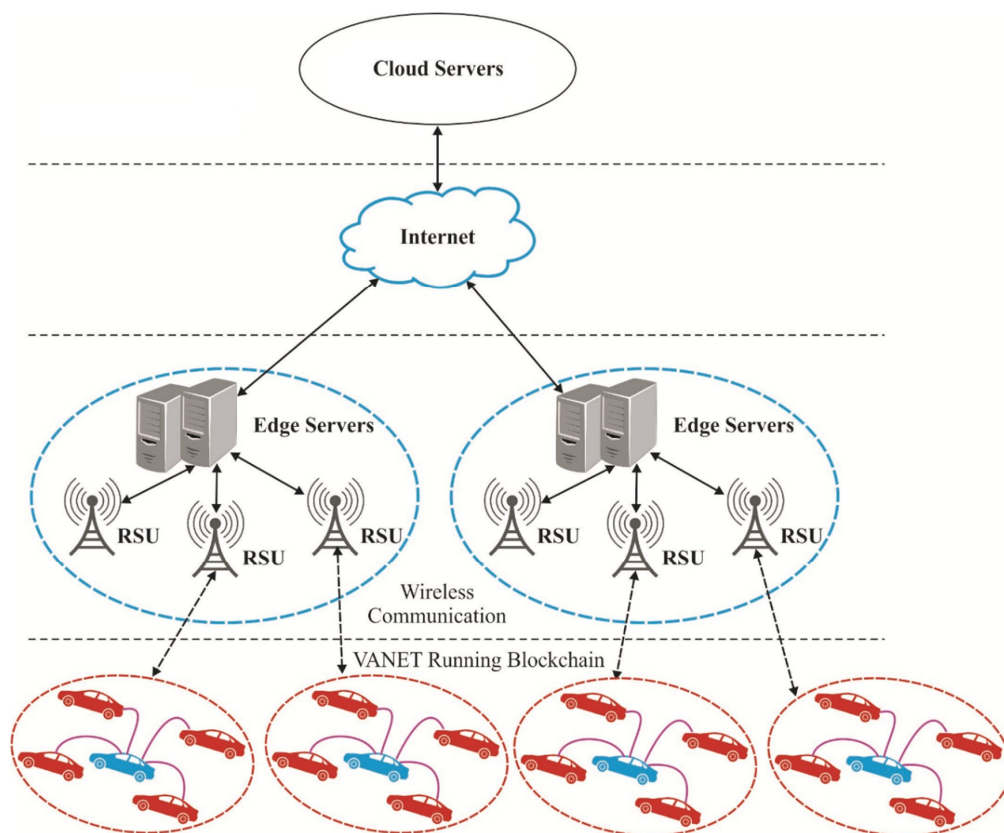
approximation, and reviewing vector determination. The Gauss–Newton iterative technique is applied for achieving maximum accuracy.

Guo et al. [23] developed a trust access authentication scheme to monitor and achieve collaborative sharing for vehicles. Besides, blockchain is used to achieve secure authentication and protected privacy. Sherazi et al. [24] focused on distributed denial of service attacks by appending the development of intrusion detection system for internet of vehicles (IoV). Besides, Artificial Intelligence (AI) and Machine Learning (ML) models are examined allowing refined defense architecture. Furthermore, a fuzzy logic and Q-learning based solution is validated to investigate the effectiveness of the presented model.

Yang et al. [25] introduced a proof-of-event consensus concept applicable to vehicular networks instead of proof-of-work or proof-of-authority techniques. The traffic data is gathered from the roadside units, and the passing vehicles ensure the accuracy on receiving the event notification. Besides, a two-phase transaction on blockchain is employed for transmitting warning messages in suitable areas. Sherazi et al. [26] developed a heterogeneous network architecture including many wireless interfaces (e.g., wireless access in vehicular environment (WAVE), long-range wireless fidelity (WiFi), and fourth generation/long-term evolution (4G/LTE)) placed on the on-board units, using the radio over fiber model for establishing the context-aware network connectivity.

### 3. The Proposed ROAC-B Technique

The proposed RAOC-B technique operates as follows. Initially, the vehicles on the road communicate with one another. Then the ROAC algorithm is executed to cluster the vehicles, and elects the CHs. Afterwards, the intercluster, intracluster, and other communication among the vehicles takes place via blockchain technology. These processes are clearly illustrated in Figure 2.



**Figure 2.** Architecture of the ROA-based clustering with blockchain-based data transmission (ROAC-B) technique.

### 3.1. ROA for Clustering in VANET

First, data is generated randomly based on parameters like node count, communication range, and grid size. After this, a network is developed from nodes in the grid. Clustering is performed according to the features of nodes, including speed, navigation, position, and so forth. To develop effective clustering, a node has to be in a single cluster. At the same time, one node can become a member in only one cluster. Each cluster has a CH, which can manage the entire cluster, and the CMs. The CH identifies the nodes entering and exiting the cluster.

At the initial stage, the vehicles are placed randomly on the highway in a 2D or 3D direction. The vehicles begin moving at a certain speed. Then the fitness of rainfall is calculated and used for cluster development. Once the iteration is completed, the location of the vehicles is updated, and new fitness measures are done to identify the effective results. Consequently, the merit order list provides optimized clusters. In this study, the ROAC technique is used to construct clusters of vehicles and to select CHs.

The natural-based models mimic the natural biological and social nature of species. The rain drop optimization (RFO) algorithm is inspired by the raindrop hierarchy [27]. Raindrops flow over a slope and form a river that finally reaches the lowest point or flows into the sea. Initially, the river is formed as a tiny stream that flows down a mountain slope. It goes around curves and folds in the land, flowing downhill. Several tiny streams emerging from raindrops meet each other and combine into the sea, which becomes higher and higher until it can be called a river. The raindrop chooses the path with the steeper slope; RFO accelerates the tendency and uses the gradient of the objective function, which calculates the solution that has to be optimized.

The locations of neighbor points of each drop are related to the drop's location prior to moving toward the neighbor point through the lowest position. This path is followed until the drop reaches a valley. When the drops are flowing high to low, overcoming massive hurdles on their way to the valley, rain drop flows and ran from puddles to maintain the valley by the proper model has been executed by the RFO algorithm. The accessibility of RFO is not a major problem, as it is a population-dependent optimization method that uses a minimization of objective function measures to compute a qualified solution from the next iteration. The proposed optimization method begins with arbitrarily produced solutions and continues successive random exploration from the preceding point for alterations of the present value until a termination condition is reached. The RFO strategy is autonomous and converges on the most optimal solution by a form of guessing. It begins with a primary solution and enhances it to identify the best solution with the maximum probability.

Figure 3 depicts the flowchart of the proposed method. Using the evolutionary models, RFO is initiated using the initial population [27].

**Raindrop:** A particle that is present in a population with variables of optimization issues, and which satisfies the problem. When the population size is  $m$ , the value of the drop  $i$  is represented in Equation (1).

$$D^i = [x_{i,1}x_{i,2}x_{i,3} \dots x_{i,k} \dots x_{i,n}] i \in \{1, 2, 3, \dots, m\} \quad (1)$$

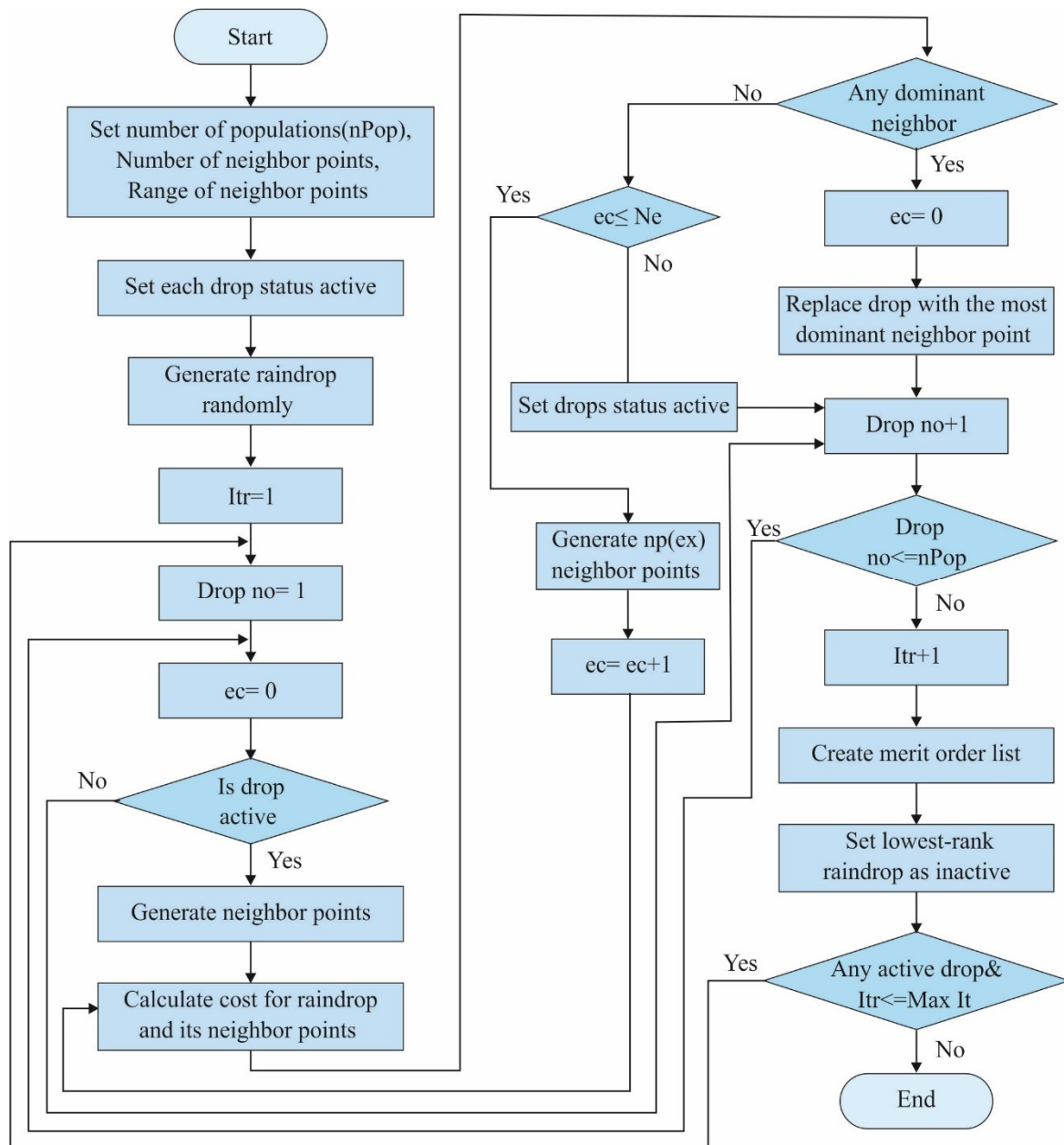
where  $n$  is the count of optimization variables;  $x_{i,k} : k^{th}$  defines the attribute of the optimization issue;  $D^i$  is the drop number  $i$ .

Notably,  $D^i$  is considered a point in  $N$ -dimensional axes, where it is defined as an  $N$ -element vector. Rainfall deals with raindrops at the time of the optimization process. It is produced based on an even random distribution function, and the limitations are shown in Equation (2).

$$x_{i,k} = U(low_k, up_k) \quad (2)$$

where  $low_k$  and  $up_k$  are the lower and upper limits of  $x_k$ ;  $U$  is the uniform distribution function.





**Figure 3.** Flowchart of the rain drop optimization (RFO) algorithm.

**Neighborhood:** As raindrop  $D$  contains  $N$  elements and represents a point in  $N$ -dimensional axes, the radius vector of  $r$  is called a neighborhood. A small modification in raindrop value changes the neighborhood value.

**Neighbor point:** A point in a drop's neighborhood is produced randomly at the time of the optimization, and neighbor point  $j$  of drop  $i$  is represented by  $NP_j^i$  as per the following equation:

$$\begin{aligned}
 &\| (D^i - NP_j^i) \cdot \hat{u}k \| \leq \| r \cdot \hat{u}k \| \\
 &i = \{1, 2, 3, \dots, m_j\} \\
 &j = \{1, 2, 3, \dots, np_j\} \\
 &k = \{1, 2, 3, \dots, nj\} \\
 &r = r_{initial} \times f(\text{Iteration})
 \end{aligned} \tag{3}$$

where  $r$  represents the real positive vector that determines the neighborhood size in  $N$ -dimensional space, and the elements are greater the greater the neighborhood size;  $r_{initial}$  is the initial neighborhood size;  $f$  is the function that applies the step size, selecting the neighborhood size in specific iterations;  $NP$  is the count of neighbor points that is produced while determining the values, and  $\hat{u}$  is the unit vector of the  $k^{th}$  dimension.

**Dominant drop:** Out of the neighbor points of drop  $D^i$ , the dominant neighbor point  $NP_d^i$  refers to a point that satisfies (4). The objective function is represented by. Hence, the functions for the drop and the neighbor points are represented by  $F(D^i)$  and  $F(NP_j^i)$ , respectively.

$$\begin{aligned} F(NP_d^i) &< F(D^i) \\ F(NP_d^i) &< F(NP_j^i) \quad j \in \{1, 2, 3, \dots, np\} - \{d\} \end{aligned} \quad (4)$$

**Active drop:** A drop that contains a dominant neighbor point.

**Inactive drop:** A drop without a dominant neighbor point.

**Explosion process:** This happens during optimization without a dominant neighbor point, when the raindrop's condition is unstable, because there are not enough neighbor points to produce a local or global minimum. After the explosion has been performed and the drop goes out of the limit, it is considered to be  $Ne$  times. The neighbor points are produced through the explosion process ( $np_{(ex)}$ ), which is computed through Equation (5).

$$np_{(ex)} = np \times eb \times ec \quad (5)$$

where  $np$  is the count of neighbor points under ordinary conditions;  $eb$  represents the explosion base that determines the range, and  $ec$  is the explosion count.

**Raindrop rank:** For all iterations of the optimization process, the range of the raindrops is determined based on Equation (6) for the application of the merit order list.

$$\begin{aligned} C1_t^i &= F(D^i) \Big|_{at \ t^{th} \ iteration} - F(D^i) \Big|_{at \ 1^{st} \ iteration} \\ C2_t^i &= F(D^i) \Big|_{at \ t^{th} \ iteration} \\ Rank_t^i &= \omega_1 \times order(C1_t^i) + \omega_2 \times order(C2_t^i) \end{aligned} \quad (6)$$

where  $C1_t^i$  is the accurate modification of the objective function from initial iteration  $t$  for raindrop  $D^i$ ;  $C2_t^i$  is the measure of the objective function for raindrop  $D^i$  at iteration  $t$ ;  $order(C1_t^i)$  and  $order(C2_t^i)$  are the orders of  $C1$  and  $C2$  at iteration  $t$  if it is arranged in increasing order;  $\omega_1$  and  $\omega_2$  are the weighting coefficients estimated as 0.5;  $Rank_t^i$  is the range of raindrop  $D^i$  at iteration  $t$ .

**Merit order list:** This is a list with raindrops in all iterations, arranged in ascending order, eliminated from the population for optimization.

Initially, raindrops are produced randomly and exceed the cost function. The proposed model is operated with possible solutions over the optimized iterations, and the possible solutions are produced through a search mechanism of this model. During the optimization process, the neighbor point overflows the search-space and restricts the outcomes of the RFO searching strategy. The neighbor point produced in the search-space is maximized with the help of the following equation:

$$if \ (NP_{ji})_k < low_k \ then \ (NP_{ji})_k = low_k \quad (7)$$

Or

$$if \ (NP_{ji})_k > up_k \ then \ (NP_{ji})_k = up_k \quad (8)$$

The measure attained for a raindrop is related to the measure of neighbor points needed to identify the dominant neighbor point. When a new number of neighbor points is produced, sufficient to resolve the issues, this is called an explosion.

The primary iteration of the RFO model is completed while similar strategies are used for raindrops. This is repeated until a large number of drops reach minimum points during the iteration. The main features of this model are the number of neighbor points, the neighborhood size, the population count, and the value of neighbor points in the explosion. Once the CH is selected, the nearby vehicles join the CH and become CMs. Thereby the cluster is constructed.

### 3.2. Blockchain-Based Secure Transmission

A blockchain is a set of blocks. Every block contains four segments: data regarding the transaction (bitcoin, ethereum), hash value of the previous block, the current block, and the timestamp. A blockchain is also defined as a distributed common electronic ledger that is used to save the transaction information using diverse points. Transactions can be recorded using a cryptographic hash value that is verified by all miners. It is held with similar values in the complete ledger, and is composed of blocks of all the transactions, as depicted in Figure 4. The blockchain provides the ability to share ledger details in a secured format [28]. Decentralized storage is a source in a blockchain, and maximum data can be recorded and transferred from the current block to the previous block using an intelligent contract code. In Swarm, LitecoinDB, MoneroDB, SiacoinDB, Interplanetary File System (IPFS), and BigchainDB, different factors are used for the decentralized database.

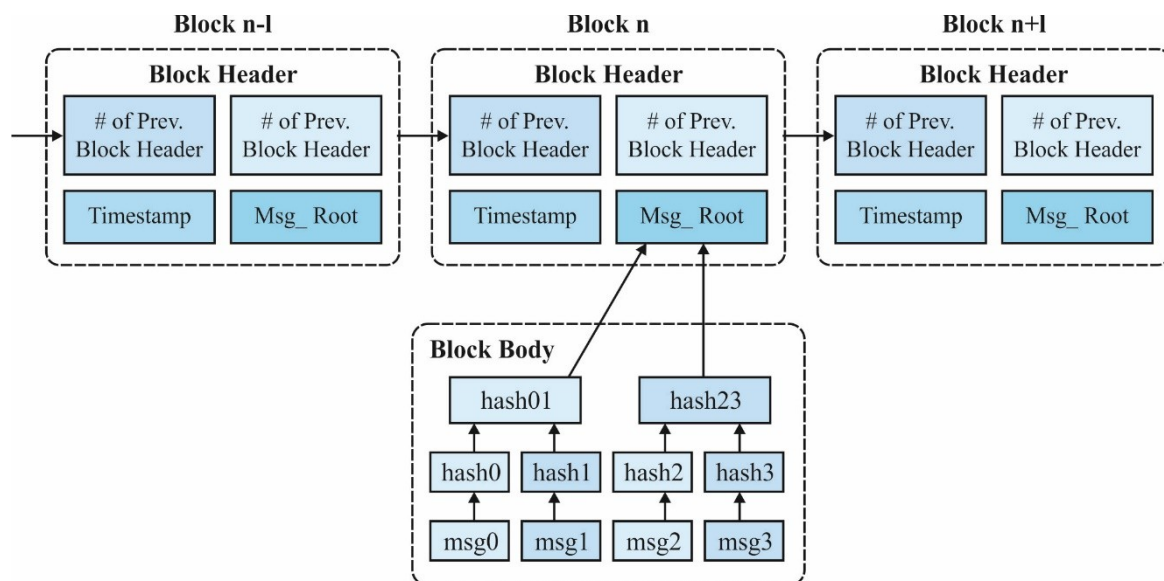


Figure 4. Structure of a blockchain.

It should be assumed that vehicles interact with one another through V2V and vehicle-to-everything (V2X) communication, and that vehicles can connect to the Internet effectively. Consider also that all vehicles are essential such as OBUs, sensors, and GPS. Moreover, the number of legitimate RSUs is higher than that of suspicious RSUs. It is assumed that crucial event messages are disseminated inside a region of interest. The message count is also essential to ensuring that the event and the message are identified as correct.

A new type of blockchain is needed, as typical blockchains cannot be used for our purpose. A traditional blockchain used is cryptocurrency, while we need a blockchain that deals with secured event messages without using crypto-coins. Therefore, it uses a safety event message as an event message. The blockchain is necessary for the trustworthiness of safety messages in a VANET. It is a single blockchain that has been balanced and supervised autonomously to record the transport details.



All vehicles telecast their positions with beacon messages. Location certificate (LC) is used as a digital proof, which represents a vehicle that is at a specified distance and within the period.

All vehicles require an LC to approve their position simultaneously. An LC is offered by a legitimate RSU. It acts as a proof of location (PoL) for vehicles, which helps to find the event messages in a given geographical area. The problems of scalability and timeliness in the previous blockchain become insurmountable for real-time VANET applications. Here, the events are local, and event messages are confined to vehicles found within a specific geographical area. In the classical blockchain, the newly minted block is broadcast universally. But the VANET messages do not cross the boundary of a specific location, since the traffic and accident details of a location are unknown to vehicles found in another location. Therefore, a new blockchain mechanism is required. From this independent blockchain, all miners mine fresh blocks according to the event messages, and forward every newly minted block to the local blockchain network. Then a vehicle can query its security level, whenever required, through the blockchain. Once the generation is completed, the new block is broadcast, and vehicles in the network validate and upgrade the blockchain.

#### 4. Performance Validation

This section discusses the performance validation of the proposed ROAC-B technique. We analyze various grid sizes in terms of packet delivery ratio (PDR), end to end (ETE) delay and throughput. The simulations are performed using the Network Simulator-2 (NS-2) version 2.35 with the mobility of vehicles generated by the simulation of urban mobility (SUMO).

##### 4.1. Parameter Settings

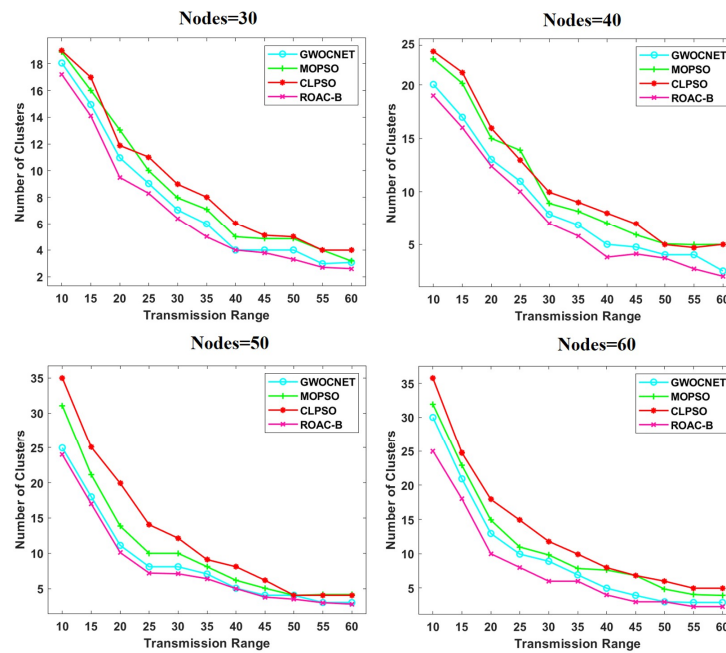
The parameter settings of the ROAC-B technique are shown in Table 1. The proposed method has been implemented using a SUMO simulator, and a detailed comparative study is given below.

**Table 1.** Parameter Settings.

Parameter	Value
Node Count	100
Max. Vehicle Speed	33 m/s
Max. Acceleration	2.6 m/s <sup>2</sup>
Max. Deceleration	4.5 m/s <sup>2</sup>
Number of RSUs	10
RSU Coverage	1 km

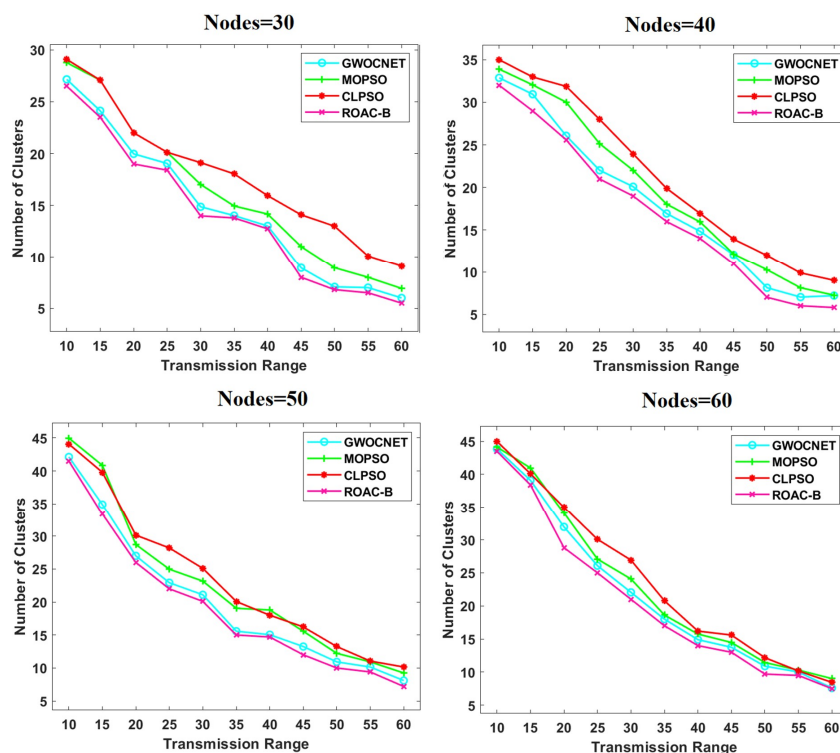
##### 4.2. Analysis of the ROAC-B Technique at Various Grid Sizes

The performance of the ROAC-B technique was validated, and we examined various aspects of the results. Figure 5 shows the number of clusters within the transmission range of  $100 \times 100$  m with a node count of 30–60. The figure shows that the proposed model has attained the smallest number of clusters at varying transmission ranges. The comprehensive learning particle swarm optimizer (CLPSO) algorithm was less effective with more clusters. The multiobjective particle swarm optimization (MOPSO) algorithm was slightly better, offering a slightly smaller number of clusters. The grey wolf optimization-based clustering network (GWOCNET) model has reached a near-optimal performance by attaining an even smaller number of clusters. Finally, the ROAC-B model has led to the best results by achieving the lowest cluster count. A lower number of clusters avoids collision and packet loss. The figure also shows that with an increased node count, the ROAC-B model has still performed best by attaining a higher number of clusters.



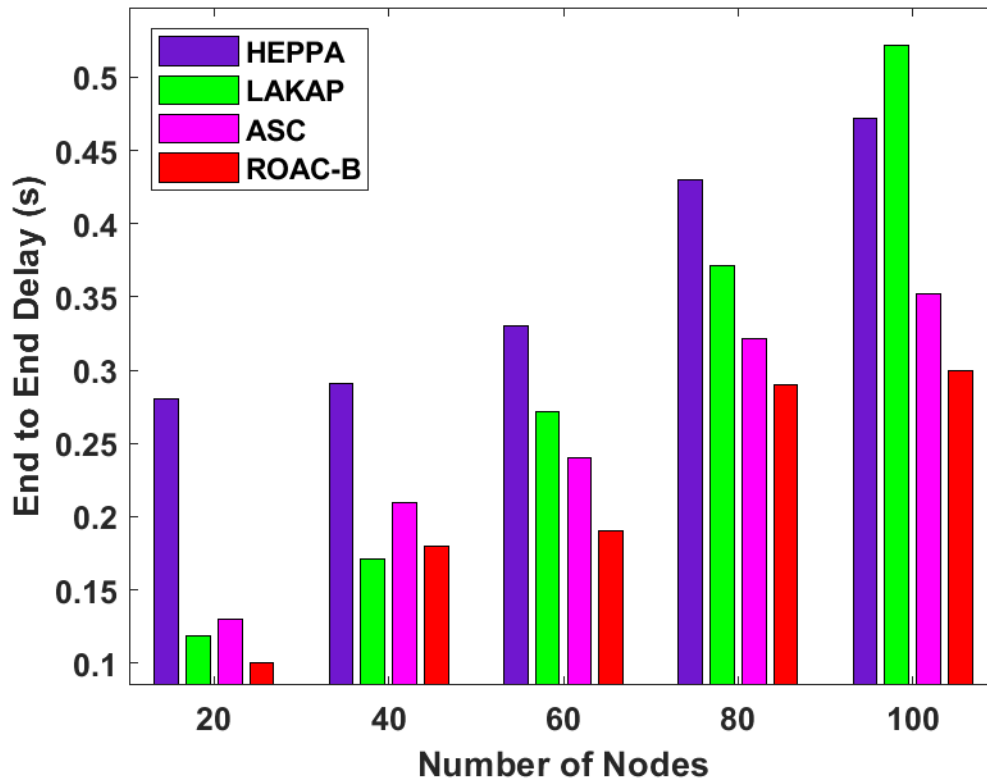
**Figure 5.** Number of clusters vs. transmission range in a 100 m  $\times$  100 m grid (Node count 30–60).

Figure 6 shows the number of clusters at the transmission range of 200  $\times$  200 m with a node count of 30–60. The figure shows that our method has achieved the smallest number of clusters at various transmission ranges. The CLPSO method was ineffective, generating a large number of clusters. The MOPSO model gave a somewhat better result by offering a somewhat lower number of clusters. The GWOCNET method performed better by obtaining an even lower number of clusters. Finally, the ROAC-B method has led to the best outcomes by attaining the smallest cluster count. The figure also shows that with an increased node count, the ROAC-B method yields the optimal performance by obtaining a higher number of clusters.



**Figure 6.** Number of clusters vs. transmission range in a 200 m  $\times$  200 m grid (Node count 30–60).

Figure 7 presents the end to end delay analysis of the ROAC-B method under a denial of service attack. The figure shows that the HEPPA and LAKAP methods have shown a higher ETE delay value than the other models. The ASC technique has yielded moderate results by obtaining a slightly lower ETE delay value. But the proposed ROAC-B technique has demonstrated a better performance by attaining the lowest ETE delay value.



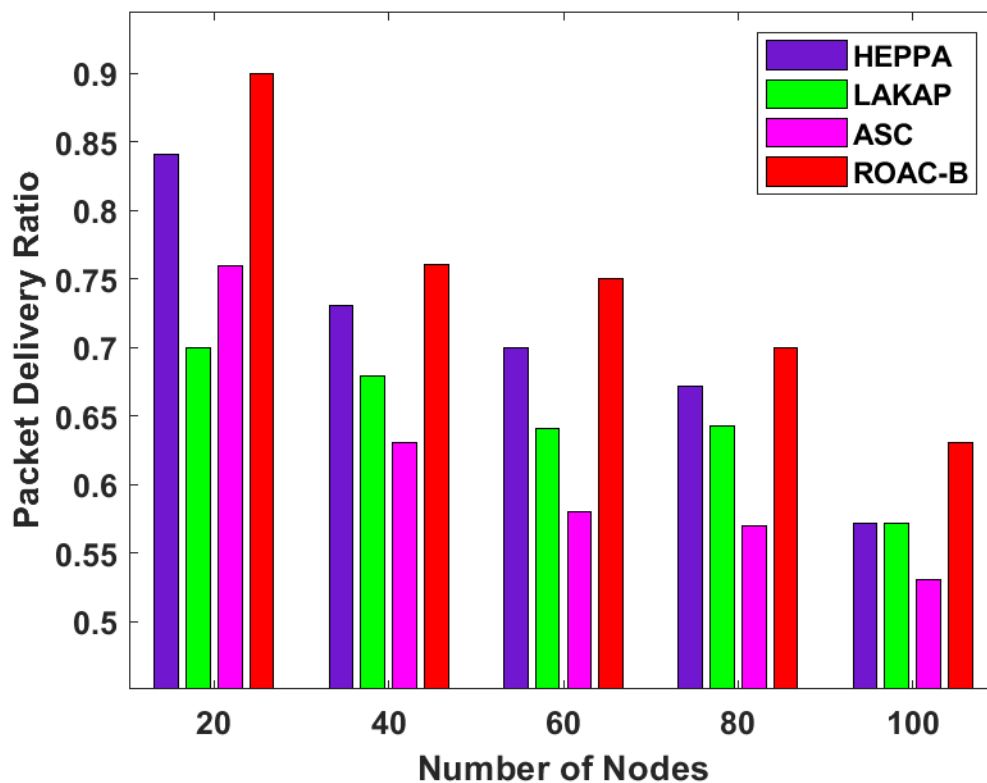
**Figure 7.** End to end (ETE) delay analysis of the ROAC-B technique. HEPPA: hybrid method for a privacy-preserving authentication approach, LAKAP: lightweight authentication and key agreement protocol, ASC: authentication scheme smart card.

#### 4.3. Analysis of the ROAC-B Technique in Terms of PDR

PDR is a ratio of the number of packets that were successfully provided to the overall number of packets forwarded. It can be calculated using the ratio of the total number of packets received,  $P_r$ , to the total number of packets transmitted,  $P_s$ , in the network, as shown in Equation (9):

$$PDR = \frac{P_r}{P_s} \times 100\% \quad (9)$$

Figure 8 presents the PDR analysis of the ROAC-B technique under a denial of service attack at varying node counts. The figure shows that the ASC and LAKAP models performed the worst and attained the lowest PDR values out of all the methods. The HEPPA technique yielded moderate results by attaining a slightly higher PDR value. However, the proposed ROAC-B technique has performed best by obtaining the highest PDR value. For instance, at a node count of 20, the presented ROAC-B technique has attained the maximum PDR of 0.9, whereas the HEPPA, LAKAP, and ASC models have resulted in lower PDRs of 0.84075, 0.7, and 0.75925.



**Figure 8.** Packet delivery ratio analysis of ROAC-B technique under a denial of service attack.

At a node count of 40, the proposed ROAC-B method yielded the highest PDR of 0.76, while the HEPPA, LAKAP, and ASC models resulted in lower PDRs of 0.73, 0.6795, and 0.63. At a node count of 60, the proposed ROAC-B model achieved the highest PDR of 0.75, while the HEPPA, LAKAP, and ASC methods resulted in lower PDRs of 0.7, 0.64075, and 0.5795. At a node count of 80, the presented ROAC-B method yielded the highest PDR of 0.7, whereas the HEPPA, LAKAP, and ASC models resulted in lower PDRs of 0.67125, 0.64225, and 0.56955. At a node count of 100, the presented ROAC-B technique has achieved the highest PDR of 0.63, whereas the HEPPA, LAKAP, and ASC methods have resulted in lower PDRs of 0.57125, 0.57125, and 0.53.

#### 4.4. Analysis of the ROAC-B Technique in Terms of Throughput

Figure 9 presents the throughput analysis of the ROAC-B method under a denial of service attack. The figure shows that the ASC and LAKAP methods have performed badly and achieved the lowest throughput values out of all the models. The HEPPA technique has yielded moderate results by obtaining a somewhat higher throughput value. But the presented ROAC-B technique has performed best by obtaining the highest throughput value.

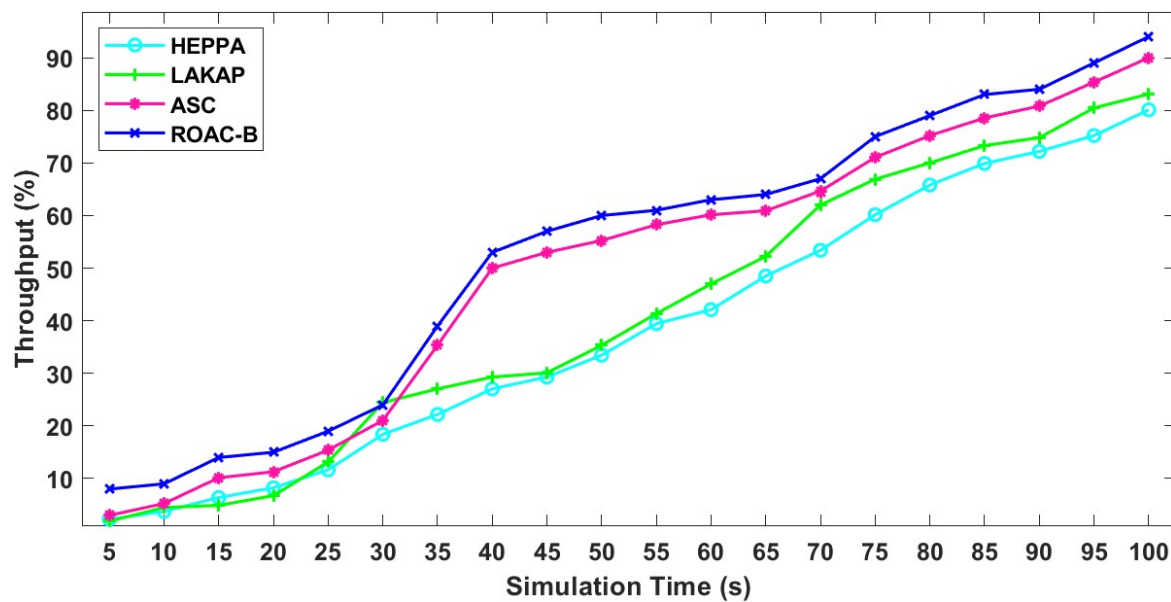


Figure 9. Throughput analysis of ROAC-B technique under a denial of service attack.

For instance, in an execution round of 10 s, the presented ROAC-B model has achieved the highest throughput of 9%, while the HEPPA, LAKAP, and ASC methods have yielded lower throughputs of 3.75%, 4.5%, and 5.25%, respectively. In an execution round of 20 s, the proposed ROAC-B technique obtained the highest throughput of 15%, but the HEPPA, LAKAP, and ASC models yielded lower throughputs of 8.25%, 6.75%, and 11.29%, respectively. In an execution round of 30 s, the proposed ROAC-B technique attained the highest throughput of 24%, whereas the HEPPA, LAKAP, and ASC models yielded lower throughputs of 18.4%, 24.45%, and 21.05%, respectively. In an execution round of 40 s, the presented ROAC-B technique achieved the highest throughput of 53%, whereas the HEPPA, LAKAP, and ASC techniques yielded lower throughputs of 27.05%, 29.3%, and 50%, respectively. In an execution round of 50 s, the projected ROAC-B model obtained the highest throughput of 60%, while the HEPPA, LAKAP, and ASC models yielded lower throughputs of 33.45%, 35.35%, and 55.25%, respectively. In an execution round of 60 s, the presented ROAC-B technique attained the highest throughput of 63%, whereas the HEPPA, LAKAP, and ASC approaches yielded lower throughputs of 42.1%, 47%, and 60.15%, respectively. In an execution round of 70 s, the proposed ROAC-B model achieved the highest throughput of 67%, while the HEPPA, LAKAP, and ASC models have yielded lower throughputs of 53.39%, 62%, and 64.65%, respectively. In an execution round of 80 s, the proposed ROAC-B technique attained the highest throughput of 79%, whereas the HEPPA, LAKAP, and ASC techniques resulted in lower throughputs of 65.8%, 70%, and 75.2%, correspondingly. In an execution round of 90 s, the proposed ROAC-B method achieved the highest throughput of 84%, whereas the HEPPA, LAKAP, and ASC models yielded lower throughputs of 72.19%, 74.8%, and 80.8%, respectively. In an execution round of 100 s, the presented ROAC-B technique attained the highest throughput of 94%, while the HEPPA, LAKAP, and ASC models yielded lower throughputs of 80.09%, 83.09%, and 90%, respectively.

## 5. Conclusions

This paper has introduced an efficient privacy-preserving data transmission architecture, incorporating blockchain technology for ensuring privacy and security in a cluster-based VANET. Initially, the vehicles on the road communicate with one another. Then the ROA algorithm is executed to cluster the vehicles, and selects appropriate CHs. Afterwards, the intercluster, intracluster, and other communication among the vehicles takes place via blockchain technology. A set of simulation processes was done to verify the efficiency of the ROAC-B technique, and several aspects of the results



were investigated. The simulation outcome suggests that the ROAC-B technique is superior to other techniques in terms of PDR, ETE delay, throughput, and cluster size. In the future, the function of the proposed method can be improved using a consensus algorithm.

**Author Contributions:** Conceptualization, G.P.J., E.P. and K.S.; Data curation, E.P. and K.S.; Formal analysis, E.P. and K.S.; Funding acquisition, U.T., T.A. and A.I.; Investigation, U.T. and T.A.; Methodology, K.S.; Project administration, G.P.J., U.T. and A.I.; Resources, U.T., T.A. and A.I.; Supervision, G.P.J.; Validation, G.P.J.; Visualization, U.T.; Writing—original draft, G.P.J.; Writing—review and editing, K.S. All authors have read and agreed to the published version of the manuscript.

**Funding:** The author(s) received financial support for the research, authorship, and/or publication of this article by Deanship of Scientific Research at Prince Sattam Bin Abdulaziz University under the research project 2020/01/16466.

**Acknowledgments:** This project was supported by the Deanship of Scientific Research at Prince Sattam Bin Abdulaziz University under the research project 2020/01/16466.

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

## References

1. Ghorl, M.R.; Zamli, K.Z.; Quosthoni, N.; Hisyam, M.; Montaser, M. Vehicular ad-hoc network (VANET): Review. In Proceedings of the 2018 IEEE International Conference on Innovative Research and Development ICIRD, Bangkok, Thailand, 11–12 May 2018.
2. Abbasi, I.A.; Khan, A.S. A review of vehicle to vehicle communication protocols for VANETs in the urban environment. *Future Int.* **2018**, *10*, 14. [CrossRef]
3. Zeadally, S.; Hunt, R.; Chen, Y.S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommun. Syst.* **2012**, *50*, 217–241. [CrossRef]
4. Qu, F.; Wu, Z.; Wang, F.Y.; Cho, W. A security and privacy review of VANETs. *IEEE Trans. Intell. Transp. Syst.* **2015**, *10*, 2985–2996. [CrossRef]
5. Engoulou, R.G.; Bellaïche, M.; Pierre, S.; Quintero, A. VANET security surveys. *Comput. Commun.* **2014**, *44*, 1–13. [CrossRef]
6. Patel, N.J.; Jhaveri, R.H. Trust based approaches for secure routing in VANET: A survey. *Procedia Comput. Sci.* **2015**, *45*, 592–601. [CrossRef]
7. Xi, Y.; Sha, K.; Shi, W.; Schwiebert, L.; Zhang, T. Enforcing privacy using symmetric random key-set in vehicular networks. In Proceedings of the Eighth International Symposium on Autonomous Decentralized Systems, Phoenix, AZ, USA, 21–23 March 2007.
8. Defrawy, K.E.; Tsudik, G. ALARM: Anonymous location-aided routing in suspicious MANETs. *IEEE Trans. Mob. Comput.* **2016**, *10*, 1345–1358. [CrossRef]
9. Prashar, D.; Jha, N.; Jha, S.; Joshi, G.P.; Seo, C. Integrating IoT and Blockchain for Ensuring Road Safety: An Unconventional Approach. *Sensors* **2020**, *20*, 3296. [CrossRef]
10. Dai, H.-N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A Survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [CrossRef]
11. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: <https://nakamotoinstitute.org/bitcoin/> (accessed on 20 April 2020).
12. Ostermaier, B.; Dotzer, F.; Strassberger, M. Enhancing the security of local dangerwarnings in vanets—A simulative analysis of voting schemes. In Proceedings of the 2nd International Conference on Availability, Reliability and Security, Vienna, Austria, 10–13 April 2007; pp. 422–431.
13. Ying, B.; Nayak, A. Anonymous and lightweight authentication for secure vehicular networks. *IEEE Trans. Veh. Technol.* **2017**, *66*, 10626–10636. [CrossRef]
14. Wazid, M.; Das, A.K.; Kumar, N.; Odelu, V.; Reddy, A.G.; Park, K.; Park, Y. Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks. *IEEE Access* **2017**, *5*, 14966–14980. [CrossRef]
15. Rajput, U.; Abbas, F.; Eun, H.; Oh, H. A hybrid approach for efficient privacy-preserving authentication in VANET. *IEEE Access* **2017**, *5*, 12014–12030. [CrossRef]
16. Tangade, S.; Manvi, S.S. Scalable and privacy-preserving authentication protocol for secure vehicular communications. In Proceedings of the 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, Bangalore, India, 6–9 November 2016.

17. Cui, J.; Zhang, J.; Zhong, H.; Xu, Y. SPACF: A secure privacy-preserving authentication scheme for VANET with CUCKOO Filter. *IEEE Trans. Veh. Technol.* **2017**, *66*, 10283–10295. [[CrossRef](#)]
18. Lei, A.; Ogah, C.; Al, E. A Secure Key Management Scheme for Heterogeneous Secure Vehicular Communication Systems. *Zte Commun. Mag.* **2016**, 111. [[CrossRef](#)]
19. Leiding, B.; Memarmoshrefi, P.; Hogrefe, D. Self-managed and blockchain-based vehicular ad-hoc networks. In Proceedings of the 2016 ACM Int. Jt. Conf. Pervasive Ubiquitous Comput. Adjunct—UbiComp, Heidelberg, Germany, 12–16 September 2016; Volume 16, p. 137140.
20. Dorri, A. BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Commun. Mag.* **2017**, *55*, 119–125. [[CrossRef](#)]
21. Rowan, S.; Clear, M.; Gerla, M.; Huggard, M.; Goldrick, C.M. Securing Vehicle to Vehicle Communications using Blockchain through Visible Light and Acoustic Side-Channels. *arXiv* **2017**, arXiv:1704.02553.
22. Song, F.; Zhu, M.; Zhou, Y.; You, I.; Zhang, H. Smart collaborative tracking for ubiquitous power IoT in edge-cloud interplay domain. *IEEE Int. Things J.* **2019**. [[CrossRef](#)]
23. Guo, S.; Hu, X.; Zhou, Z.; Wang, X.; Qi, F.; Gao, L. Trust access authentication in vehicular network based on blockchain. *China Commun.* **2019**, *16*, 18–30. [[CrossRef](#)]
24. Sherazi, H.H.R.; Iqbal, R.; Ahmad, F.; Khan, Z.A.; Chaudary, M.H. DDoS attack detection: A key enabler for sustainable communication in internet of vehicles. *Sustain. Comput. Inf. Syst.* **2019**, *23*, 13–20. [[CrossRef](#)]
25. Yang, Y.T.; Chou, L.D.; Tseng, C.W.; Tseng, F.H.; Liu, C.C. Blockchain-based traffic event validation and trust verification for VANETs. *IEEE Access* **2019**, *7*, 30868–30877. [[CrossRef](#)]
26. Sherazi, H.H.R.; Khan, Z.A.; Iqbal, R.; Rizwan, S.; Imran, M.A.; Awan, K. A heterogeneous IoV architecture for data forwarding in vehicle to infrastructure communication. *Mob. Inf. Syst.* **2019**. [[CrossRef](#)]
27. Moazzeni, A.R.; Khamsehchi, E. Rain optimization algorithm (ROA): A new metaheuristic method for drilling optimization solutions. *J. Pet. Sci. Eng.* **2020**, 107512. [[CrossRef](#)]
28. Shrestha, R.; Bajracharya, R.; Shrestha, A.P.; Nam, S.Y. A new type of blockchain for secure message exchange in VANET. *Digit. Commun. Netw.* **2020**, *6*, 177–186. [[CrossRef](#)]



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).