sustainability

MDPI

Article

A Blockchain-Assisted Trusted Clustering Mechanism for IoT-Enabled Smart Transportation System

Kamran Ahmad Awan [1], **Ikram Ud Din** [1,*] and **Ahmad Almogren** [2,*]

[1] Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[2] Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
* Correspondence: ikramuddin205@yahoo.com (I.U.D.); ahalmogren@ksu.edu.sa (A.A.)

Abstract: Vehicular Ad-hoc Network (VANET) is a modern concept of transportation that was formulated by extending Mobile Ad-hoc Networks (MANETs). VANET presents diverse opportunities to modernize transportation to enhance safety, security, and privacy. Direct communication raises various limitations, most importantly, the overhead ratio. The most prominent solution proposed is to divide these nodes into clusters. In this paper, we propose a clustering mechanism that provides security and maintains quality after the cluster formulation based on the pre-defined Quality-of-Service (QoS) parameters. To address potential attacks in the VANET environment, the proposed mechanism uses blockchain to encrypt the trust parameters' computation. A particular trust degree of a vehicle is evaluated by the base station, encrypted with the blockchain approach, and transmitted toward roadside units (RSUs) for further utilization. The system's performance is evaluated and compared with the existing approaches. The results show a significant improvement in terms of security and clustering quality.

Keywords: VANET; blockchain; Internet of Things; Quality-of-Service; trust management; security; clustering; Intelligent Transport System; Integrity

check for updates

Citation: Awan, K.A.; Din, I.U.; Almogren, A. A Blockchain-Assisted Trusted Clustering Mechanism for IoT-Enabled Smart Transportation System. *Sustainability* **2022**, *14*, 14889. https://doi.org/10.3390/su142214889

Academic Editor: Pan Lu

Received: 27 September 2022
Accepted: 8 November 2022
Published: 11 November 2022

1. Introduction

Vehicular Ad-hoc Network (VANET) is a concept that can enhance the transportation system. The important aspect of VANET is Intelligent Transport System (ITS). ITS is an advanced application of VANET that provides several ways to maintain traffic and facilitate vehicles on roads [1]. The integration of ITS into VANET provides several precedences, i.e., road safety [2], driver destination awareness [3], and notable advancement in control mechanics with advanced communication technologies, sensing, and computation. The architecture of VANET consists of a base station, roadside units (RSUs), and vehicles, as shown in Figure 1 [4]. The base station is a centralized controlling station that controls and coordinates all the activities of the VANET and acts as a backbone, whereas RSUs facilitate vehicles in the dissemination of messages and help the base station to lighten the burden. Furthermore, the same issue is faced by VANET nodes in smart cities, whereas *the authors of* [5] discuss several communication challenges. The VANET environment also provides communications facilities that consist of Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Infrastructure-to-Infrastructure (I2I) communications.

The communication among infrastructure and network participation nodes has several drawbacks [6,7]. Most importantly, it creates communication overhead on the infrastructure. When the VANET infrastructure receives an enormous amount of requests from vehicles, the response time may increase, which results in a higher overhead ratio. To address the challenges associated with overhead and limitations caused by it, researchers have proposed a clustering mechanism [8] in which vehicles group together to form a cluster. The cluster is led by the cluster head [9], and the cluster's participating nodes are only allowed to communicate with the head. However, cluster heads are allowed to communicate with the infrastructure to reduce the overhead and enlighten the burden with the help of other cluster heads. There are several approaches that have been proposed to formulate a cluster based on different parameters, as discussed in Section 2. The prologue of formulating a cluster that maintains security, privacy, integrity, QoS, and the identification of malicious and compromised nodes concurrently required notable attention. To date, no such mechanism has been proposed to address all the limitations concurrently. In this paper, we have proposed a clustering mechanism that can maintain security [10], integrity [11] and quality [12] concurrently as well as provide adequate resilience to address the clustering challenges. To maintain security, the proposed mechanism uses blockchain [13] to encrypt sensitive information related to vehicles, i.e., trust degree and QoS [14], in terms of predefined parameters. The encrypted information is saved by the base station for propagation and aggregation to eliminate the successful execution of numerous potential attacks in the VANET environment. The trust parameters are used in the proposed mechanism for the successful identification and elimination of malicious nodes [15], whereas the Quality-of-Service (QoS) parameters are being utilized to maintain the quality after the cluster formulation. The major contributions of the proposed mechanism can be summarized as follows.

- An infrastructure-less approach is used to maintain security and privacy as well as provide a trustworthy environment to the mobile VANET nodes to utilize the maximum benefits of ITS applications for driver safety.
- The utilization of blockchain technology to maintain security and integrity along trust management parameters to identify malicious and compromised nodes.
- A novel integration of QoS evaluation with trust computations to formulate and managed clustering mechanisms with backup heads with enhanced responsibilities to achieve scalability and efficiency.
- The computations of mean opinion score evaluated by the backup heads of clusters to maintain the ratings of clusters heads that will help to increase the quality within clusters.

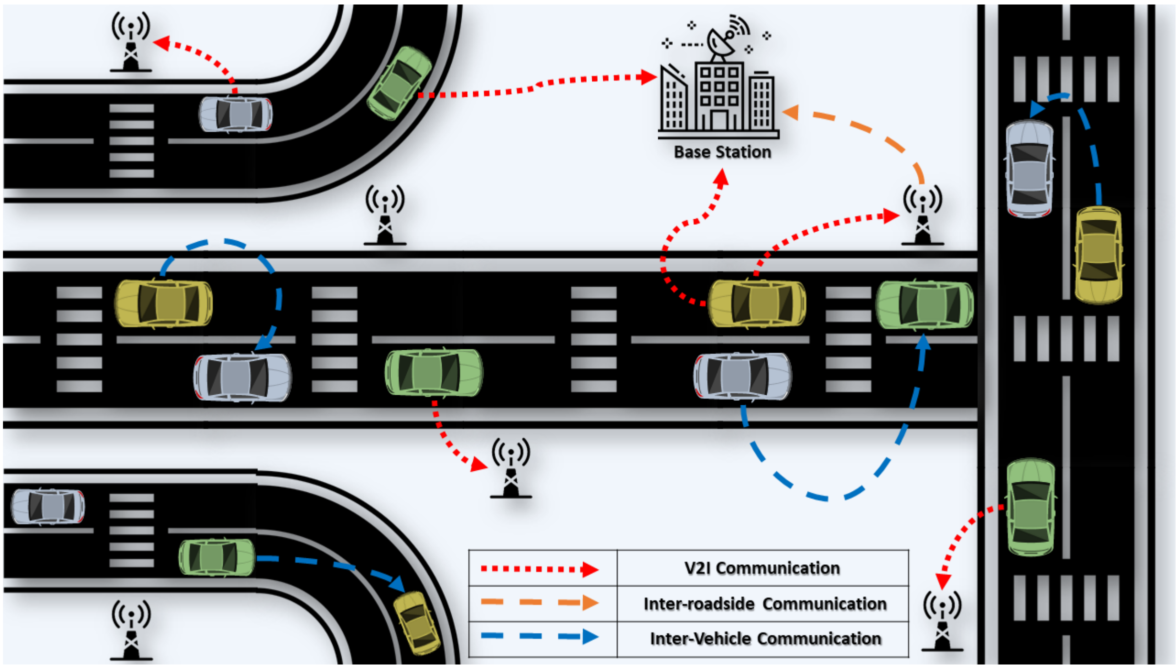

Figure 1. The architecture of Vehicular Ad-hoc Network.

The structure of the rest of the article is as follows. Section 2 elaborates on the existing clustering approaches. Section 3 explains the proposed clustering mechanism and its architecture. Section 3.1 describes the utilization of blockchain, Trust, and QoS parameters. Section 4 discusses the comparative simulation results. Finally, Section 5 concludes the paper.

2. Literature Review

Several approaches have been proposed to address the challenges and weaknesses associated with V2V, V2I, and I2C communication by utilizing the concept of clustering [16]. It is one of the prominent ways to lighten the communication burden on each node to enhance the performance and reduce the vulnerabilities caused by restricting the nodes' communication. The implementation of a 5^{th} Generation network may reduce the communication burden due to the higher transmission speed and several wireless communication technologies [5]. This section discusses the existing approaches to formulate and manage clusters along with their contribution and limitation that is also illustrated by Table 1.

To address the energy and optimal routing challenges for communication in VANETs, the clustering model has been proposed [17]. The K-Medoid-based clustering approach identifies the energy-efficient nodes for irresistible communication among nodes. The proposed K-Medoid clustering algorithm consists of four steps; i.e., the initialization phase chooses the K value whereas K is the initial medoid that represents the number of clusters. The next phase consists of medoid selection, which is calculated by computing the distance between two particular points whereas medoids in this stage are the object of a cluster or a cluster within the data set. In the third phase, the cluster is formulated by utilizing the closest medoid value from each object. After formulation, the cluster head selection relies on speed, position, and acceleration, whereas a vehicle with the least distance among formulated clusters is selected as a cluster head. The major contribution of the proposed approach is the utilization of a medoid to formulate clusters, whereas cluster head selection criteria do not consider the resource-rich node and managing capabilities that may reduce the average cluster time, performance of cluster nodes along with increased end-of-end packet delivery time [18].

In [19], the study analyzes the energy saving for parked nodes and utilizes them as relay nodes to provide services for the efficient utilization of energy resources. The working mechanism of the proposed approach is divided into two parts; i.e., clusters of mobile nodes can utilize the parked nodes as relay nodes for communication and the utilization of external factors to achieve the efficient utilization of energy resources. The proposed mechanism also pre-defined the threshold value to control the energy utilization of parked vehicles to avoid stored energy depletion. The proposed approach considered different scenarios to elaborate the importance of parked vehicle utilization to cover the large area for communication when nodes are not in the communication range. The major contribution of the proposed approach is the utilization of parked vehicle resources for communication to ensure packet delivery that reduces data loss. However, it is also important to elaborate related to incentives given to the vehicle owner when they are allowed to utilize the vehicle resources. It is also significant that the resource utilization of parked vehicles can increase the chances of successful execution of Denial-of-Service (DOS) [20] or Distributed DOS attacks [21].

A deep learning-based dynamic and stable cluster head mechanism (DL-SCHS) has been proposed for VANET [22]. The study stated that it is significant to address the cluster head selection challenges as it plays an important role in the robustness of a network alongside scalability. The study also elaborated that it is significant to maintain the four metrics in cluster head selection, i.e., benefit factor, community neighborhood, trust, and eccentricity. The proposed approach uses the long short-term memory (LSTM) algorithm of a deep recurrent learning network [23] to train nodes for the detection of signals and noisy conditions. The proposed system model consists of a cluster head, cluster member, and roadside unit. The cluster members can only communicate with the cluster head, and the cluster head does have the capability for inter-cluster communication using the roadside unit (RSU). The vehicle information stored consists of a vehicle ID, speed, and distance. The significant contribution of the proposed approach is the utilization of previous and current sensing events as a sequence of input to train the LSTM model. However, it is significant to include the evaluation of nodes' capabilities and available resources before the nodes are selected as cluster heads. The capabilities will provide the competence evaluation of nodes to coordinate the cluster's members.

Another intelligent approach that has been proposed focuses on cluster optimization using a bio-inspired Whale Optimization Algorithm for VANET (WOACNET) [24]. The study stated that VANET is a significantly heterogeneous network due to the high mobility that creates several potential challenges such as the network's physical layout, reliable and stable V2V communication, and transmission range. The proposed approach utilizes the bio-inspired WOA algorithm and compares the proposed approach with other state-of-the-art bio-inspired algorithms: Gray Wolf Optimization (GWO) [25] and Ant Lion Optimization (ALO) [26]. The proposed approach starts working by selecting the individuals for initialization and then calculating the population or solution space. The third step is the selection mechanism which is followed by the evaluation function that evaluates the fitness. The approach computes the fitness of individuals with maximum iteration and updates the fitness value for each agent. At last, the approach computes the best candidate solution that will serve as maximizing functions for coming solutions. For cluster head selection, the proposed approach first calculates the distance of each vehicle with others and the best search agent (search space) that will be selected as cluster head. The approach calculates the fitness of each vehicle after a specific interval of time and updates the cluster head that contains maximum fitness. The significant contribution of the proposed mechanism is the utilization of WOA that helps in cluster optimization and enhances the performance in comparison to ALO and GWO. However, the selection criteria of cluster head neglected the evaluation of security regarding how the head manages the execution of a Sybil attack among other potential attacks of VANET. The proposed approach also formulated the mesh topology [27] that is difficult to manage and may increase the communication burden within the clusters.

Table 1. Contributions and limitations of the existing approaches.

Ref.	Contributions	Limitations
[17]	The utilization of a medoid to formulate clusters and address the energy and optimal routing challenges.	The cluster head selection does not contain the evaluation of capabilities of nodes to manage clusters alongside security.
[19]	The utilization of parked vehicle resources to transmit packets toward a destination with a pre-defined threshold value to battery energy resources utilization.	Increases the chances of DOS and DDOS attacks on parked vehicle resources.
[22]	The utilization of LSTM along with previous and current sensing events to train the VANET node for prediction.	The available resources evaluation of nodes to evaluate the competence of handling the cluster member.
[24]	The utilization of WOA for intelligence cluster creation with maximum fitness calculated with several iterations.	The creation of mesh topology increases the cost and communication burden. Calculation of fitness with multiple fitness may also increase the energy consumption.
[28]	A secure cluster formulation using trust components to maintain secure, trustworthy and privacy-aware environment.	Distinct calculation of the degree of trust during formulation and selection may increase the computation burden.

Another clustering approach has been proposed that focuses on maintaining security as a priority during the formulation of clusters and during cluster head selection named *StabTrust* [28]. The study stated that the VANET framework provides V2V, V2I, and I2I communication that increases the burden and increases the percentage of success attack execution, and clustering is introduced as an alternative to restricting the communication.

The study also elaborated that many approaches have been proposed, but most of them neglected the aspect of security during the cluster head selection, and after the creation of a cluster, it is significant to identify the malicious and compromised nodes. The proposed mechanism utilizes the trust components, i.e., knowledge, reputation, and experience to evaluate the trustworthiness of VANET nodes that want to be a cluster member or head. The approach proposed three algorithms for the evaluation of trust, i.e., trust calculation during cluster formation, degree of trust evaluation for the selection of cluster and backup heads, and evaluation of the indirect trust of a particular node when RSU does not have any direct observation to calculate trust. The major contribution of the proposed mechanism is the secure formulation of trust and selection of cluster heads by evaluating the trustworthiness of nodes to maintain a secure and privacy-aware environment. However, calculating the trust to formulate the cluster and again trust calculation for the cluster head selection may increase the computation burden on RSU that may cause vulnerabilities and delays in computations.

3. Proposed Clustering Mechanism

The communication overhead causing increased V2V, V2I, and I2I communication is one of the significant challenges, and the most prominent solution to this problem is clustering. The vehicles are grouped together to make clusters that reduce the communication burden from infrastructure. I2I communication is also possible, but their communication created less burden as compared to V2V or V2I. Reducing the communication overhead caused by vehicles' communication enhances the performance and response time of the VANET environment. Several clustering approaches have been proposed as discussed in Section 2, but most of them focus on the formulation of clusters or on security in particular. There is a requirement that such an approach enables usable security along with capabilities to maintain quality, privacy, and the elimination of malicious and compromised nodes in parallel. The proposed approach (BlockTrust) addresses previously mentioned challenges by merging the state-of-the-art blockchain approach to encrypt information to maintain integrity. BlockTrust also integrated QoS to maintain quality in clusters by selecting the higher resource node. Furthermore, the QoS evaluation merges with trust parameters evaluation to fulfill the challenges of quality, security, and integrity in parallel. The primary purpose of using trust in the proposed approach is to identify the trustworthiness of VANET nodes. The nodes can only join the clusters when they satisfy the minimum criteria of a threshold value. Another significance of BlockTrust is that it is an infrastructure-less approach and maintains the requirement of VANET by utilizing its own architecture, as illustrated in Figure 1. The proposed approach utilizes a base station for blockchain-based encryption and RSU for acting as a middle authority in addition to coordinating directly with cluster heads. Another major responsibility of RSUs is to maintain the list of such nodes that behave maliciously and also broadcast their identity to the surroundings RSUs for maintaining trustworthiness.

The proposed architecture consists of several layers in which the first layer contains a number of nodes that formulate clusters after entering into the VANET environment. The first layer is directly connected with the second layer that provides the communication capabilities, i.e., V2V, V2I, I2I, and roadside unit. The most significant layer is the third layer in which blockchain, QoS, and the trust parameters evaluation process are integrated. In the proposed architecture, the base station is the most significant entity, which communicates with roadside units to maintain trustworthiness in the environment. RSUs initiate the clustering process and assist as a front authority to nodes. The RSU requests the base station to start the evaluation process by first computing the trust degree. After completion of the trust evaluation process, the base station compares the trust degree with the threshold value for decision making. The process for the selection of cluster heads begins by computing QoS parameters and merging them with pre-evaluated trust degrees for final selection. The computed trust degree is encrypted using blockchain to maintain the integrity and enhance the accuracy of detection. The discussed working process of the proposed architecture is also illustrated by Figure 2.

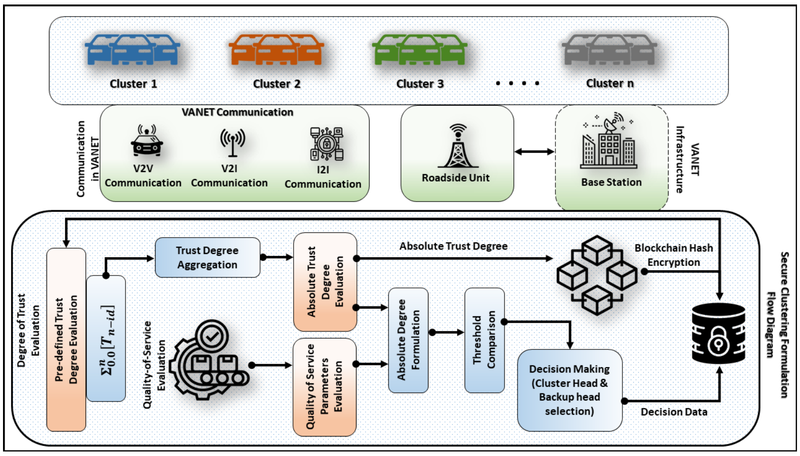
Cluster 1
Cluster 2
Cluster 3
. . . .
Cluster n
Communication in VANET
VANET Communication
V2V Communication
V2I Communication
I2I Communication
Roadside Unit
Base Station
VANET Infrastructure
Degree of Trust Evaluation
Pre-defined Trust Degree Evaluation
$\Sigma^{n}_{0.0}[T_{n-id}]$
Trust Degree Aggregation
Quality-of-Service Evaluation
Absolute Trust Degree Evaluation
Quality of Service Parameters Evaluation
Absolute Trust Degree
Absolute Degree Formulation
Threshold Comparison
Blockchain Hash Encryption
Decision Making (Cluster Head & Backup head selection)
Decision Data
Secure Clustering Formulation Flow Diagram

Figure 2. The Proposed Blockchain and QoS-Based Trusted Clustering Mechanism.

3.1. Integration of Blockchain, QoS, and Trust

Blockchain is state-of-the-art technology to encrypt information by applying HASH, in which modification becomes challenging. This technology creates an immutable ledger to maintain the integrity that will provide the ability to validate data that have been modified. In the proposed approach, blockchain is deployed to the base station that encrypts the computations performed during the creation of clusters. Implementing blockchain in the base station will decrease the computation overhead from RSUs. The encryption performed by the base station consists of a trust degree and QoS evaluation of the particular node. The encrypted data are stored using a unique identity of the node. These unique identities act as a primary key to fetch the record whenever required. These findings can be further stored in the base station database for propagation and aggregation. The encrypted data are then shared with the neighboring base station to formulate a chain of information for validation. Furthermore, the information chains are also shared with the neighboring base stations to make the VANET trustworthy. In addition, the decentralized nature of blockchain provides VANET with the capability to enhance the accuracy. This encrypted information will be shared by the base station with RSUs when required during cluster formulation.

The trust parameters and QoS have been integrated into the proposed mechanism to maintain security and quality. The trust parameters help the environment maintain security and QoS provides the quality that is required to manage the performance of a cluster. The trust parameters that are utilized in the proposed mechanism belong to the reputation component of trust, i.e., cooperativeness, honesty, and reliability. The trust computation is performed by the base station when nodes request RSU to join the cluster. Nodes will only allow joining a cluster when the trust degree is higher than the threshold value. The cooperativeness trust parameters enhance the cooperation, and the evaluation of this parameter is computed by evaluating the degree of collaboration about a particular node. Honesty is the key parameter, as it provides the capabilities to enhance the level of credibility. The honesty parameter is also inter-related with cooperativeness, which means if the nodes have a higher level of honesty, then it will also increase the level of cooperativeness. The reliability trust parameter is an important parameter in the formulation of clustering, as it delivers how efficiently the nodes can perform if it is selected as a cluster head. The reliability in the proposed mechanism is calculated by the number of operations divided by the number of failures that nodes face whenever they become a cluster head. The QoS parameters have also been integrated into the proposed mechanism to provide quality. The evaluation of QoS parameters will only be performed by the proposed mechanism when a particular node becomes a candidate of a cluster head. The QoS parameters consist of a packet delivery ratio to facilitate communication, execution time to evaluate the response rate, and mean opinion score (MOS) that is provided by backup heads of the cluster. In the proposed approach, the QoS parameters are merged into trust parameters during the cluster head selection, and the computed absolute value is used for the decision making.

3.2. Cluster Formulation and Trust Evaluation

The cluster formulation begins when a node requests the nearby RSU to join the cluster. If the cluster is available near a requested node, then RSU requests the base station to evaluate its trust degree. After trust computations, the base station shared the decision with RSU to assign that node to a cluster head for joining. If the node trust value is one node above the threshold, then that node is not able to join the cluster. If a newly joined node requests RSU to join a cluster, then a default trust degree is assigned to that node, and a node can join the nearby cluster. To overcome the communication overhead, if a node trust degree is below the threshold, then that node cannot generate any request for the next fifteen minutes. When a node requests nearby RSU to join the clusters, then RSU will evaluate the trust degree based on cooperativeness, honesty, and reliability. The process of trust evaluation begins by assigning a unique identity to the nodes. The evaluation of any parameters relies on the previous observations. The complete flow process of direct trust degree evaluation is illustrated by Algorithm 1, whereas the description of the symbols is represented by Table 2.

Algorithm 1 Direct Trust Degree Evaluation.

```
 1: procedure INITIAL NODE CHECKING($n_{id}$)
 2:     Node ID checking
 3:     Check available observation using Node ID
 4:     If no observation available, then check if it newly joined
 5:     If node is newly joined, go to step 22
 6:     Go to Indirect Evaluation if node is old but observation is not available
 7: procedure TRUST OBSERVATIONS GATHERING
 8:     Cooperativeness observations as Equation (1)
 9:     Honesty observations as Equation (3)
10:     Reliability observations as Equation (5)
11: procedure DIRECT TRUST PARAMETER EVALUATION
12:     Cooperativeness trust evaluation as Equation (2)
13:     Honesty trust evaluation as Equation (4)
14:     Reliability trust evaluation as Equation (6)
15: procedure DIRECT TRUST DEVELOPMENT
16:     Direct trust development of parameter as Equation (7a)
17:     Gathering of past trust as Equation (7b)
18:     Aggregation of current and past trust as Equation (7c)
19: procedure DECISION MAKING
20:     If trust degree $\leq 0.5$ then no trust
21:     If trust degree $\geq 0.6$ then trustworthy
22:     If newly join node, assign default trust
23: Exit
```

Table 2. Mathematical Symbols.

Symbols	Description
ct	Cooperativeness trust observations
n_{id}	Node identity
h	Honesty
re	Reliability trust evaluation
ab	Absolute trust of parameter
t	Trust
d_{tr}	Trust development
p_{tr}	Previous trust degree
a_{tr}	Absolute trust degree
rec	Indirect trust evaluation
pdr	Packet delivery ratio
c_{id}	Cluster identity
$packet_{n_{id}}^{rec}$	Packet received
$packet_{n_{id}}^{sen}$	Packet transmitted
et	Execution time
I	Instruction count
R_n	Individual rating
ab	Absolute aggregation
n	Number of observations

Firstly, the base station fetches the previous observation of cooperativeness from the database whereas the extracting process is illustrated by Equation (1).

$$ct_{n_{id}}^{cp} = ob_{n_{id}}^{cp_1} + ob_{n_{id}}^{cp_2} + \ldots + ob_{n_{id}}^{cp_n} \tag{1}$$

In Equation (1), ct represent the observations of cooperativeness trust, n_{id} shows the node identity whereas $ob_{n_{id}}^{1\ldots n}$, and cp shows the number of available observations in the database and cooperativeness, respectively. After fetching the observations, the next process is to apply the summation function on these to formulate the absolute value of cooperativeness trust degree as illustrated by Equation (2).

$$ct_{n_{id}}^{ab} = \sum_{0.0}^{n-1} \left[ob_{n_{id}}^{1} + ob_{n_{id}}^{2} + \ldots + ob_{n_{id}}^{n} \right] \tag{2}$$

In Equation (2), $ct_{n_{id}}^{ab}$ is the cooperativeness trust degree of a particular node and ab represents the absolute formulation of trust degree. The summation function is applied to available observations to compute the degree. The next step of trust evaluation is to evaluate the degree of honesty in which RSU again fetches the past observations using the node novel identity.

$$h_{n_{id}}^{tr} = ob_{n_{id}}^{ht_1} + ob_{n_{id}}^{ht_2} + \ldots + ob_{n_{id}}^{ht_n} \tag{3}$$

In Equation (3), h represents honesty evaluation, h_{id} represents the unique ID of a node, whereas $ob_{n_{id}}^{1...n}$ shows the available observations related to the particular node. After gathering the honesty observation of trust, the mechanism applies a summation function on these observations to formulate the trust degree of honesty as illustrated by Equation (4).

$$ht_{n_{id}}^{ab} = \sum_{0.0}^{n-1} \left[ob_{n_{id}}^{1} + ob_{n_{id}}^{2} + \ldots + ob_{n_{id}}^{n} \right] \tag{4}$$

In Equation (4), ht represents the trust evaluation of the honesty parameter, n_{id} shows the unique ID of a node, and ab represents the absolute trust degree of honesty. The completion of honesty trust leads the process to the evaluation of reliability evaluation of a node by first collecting the previous observations as illustrated by Equation (5).

$$re_{n_{id}}^{tr} = ob_{n_{id}}^{re_1} + ob_{n_{id}}^{re_2} + \ldots + ob_{n_{id}}^{re_n} \tag{5}$$

In Equation (5), re represents reliability, tr shows the trust evaluation of reliability whereas $ob_{n_{id}}^{re_{1...n}}$ represents the available pre-stored direct observations of reliability that can be used in the direct trust evaluation of a particular node. After gathering the observation, the approach will now apply a summation function as illustrated by Equation (6).

$$re_{n_{id}}^{ab_{tr}} = \sum_{0.0}^{n-1} \left[ob_{n_{id}}^{1} + ob_{n_{id}}^{2} + \ldots + ob_{n_{id}}^{n} \right] \tag{6}$$

Equation (6) shows the summation of reliability parameters in which re, ab, and tr represent reliability, absolute trust degree, and trust, respectively, whereas $ob_{n_{id}}^{1...n}$ shows the observations on which the summation function is applied to formulate the value. The evaluation of the reliability parameter completes the process of trust evaluation. The next phase is to develop the computed values and formulate a single trust value for decision-making. Equation (7) shows the computation of trust development in which the proposed mechanism first formulates the single value from the pre-computed trust parameter and then applies a summation function to compute the final trust value.

$$t_{n_{id}}^{d_{tr}} = ct_{n_{id}}^{ab} + ht_{n_{id}}^{ab} + re_{n_{id}}^{ab_{tr}} \tag{7a}$$

$$t_{n_{id}}^{p_{tr}} = \sum_{0.0}^{n-1} \left[pt_{n_{id}}^{ob_1} + pt_{n_{id}}^{ob_2} + \ldots + pt_{n_{id}}^{ob_n} \right] \tag{7b}$$

$$t_{n_{id}}^{a_{tr}} = \sum_{0.0}^{n-1} \left[t_{n_{id}}^{d_{tr}} + t_{n_{id}}^{p_{tr}} \right] \tag{7c}$$

In Equation (7a), t represents trust, d_{tr} shows the development of trust, whereas $ct_{n_{id}}^{ab}$, $ht_{n_{id}}^{ab}$, and $re_{n_{id}}^{ab_{tr}}$ show the cooperativeness, honesty, and reliability absolute trust values, respectively.

As mentioned earlier, the proposed mechanism also has the capability of aggregation in which the previous trust values are used by the approach to compute the aggregated trust value. The gathering process of previously computed trust degrees of a particular node is shown by Equation (7b) in which t is trust, p_{tr} is previous trust degree, and $pt_{n_{id}}^{ob_1}$ represents a single previous trust degree related to a particular node. To complete this trust aggregation process, the proposed mechanism applies the summation to the direct trust computation illustrated by Equation (7a), and to the previous trust degree computation illustrated by Equation (7b). Equation (7c) shows the aggregation process in which t is trust, a_{tr} represents absolute trust whereas $t_{n_{id}}^{d_{tr}}$ and $t_{n_{id}}^{p_{tr}}$ represent direct trust parameter computations and aggregated past trust value, respectively. This computed trust value is now further used to compare with the threshold value for decision-making.

$$\phi_{td} = \begin{cases} \text{if } t^{a_{tr}}_{n_{id}} \leq 0.5 \rightarrow NoTrust \\ \text{if } t^{a_{tr}}_{n_{id}} \geq 0.6 \rightarrow Trustworthy \\ \text{if } n_{id} = new \rightarrow Defaulttrust \end{cases} \tag{8}$$

Equation (8) illustrates the conditions of decision making in which if the final trust degree of a particular node is ≤0.5, then the node is listed as not trustworthy, i.e., no/zero trust. If the trust degree of nodes is ≥, then these nodes are listed as trustworthy and become a part of an existing cluster. However, if no clusters are available in their surroundings, then nodes can also initiate the process of cluster formulation. The third scenario is the default trust degree, which is only assigned to the newly joined nodes. When a node newly joins the network, then no pre-existing observations are available related to such nodes in which case the default degree of trust is assigned to these nodes.

As illustrated in the proposed architecture by Figure 2, the proposed approach also integrates the blockchain [29] capabilities to provide integrity to the trust degree. RSUs act as a front authority that communicates with the vehicle to maintain and coordinate with the node, whereas the base station is the primary authority that performs trust evaluations and transmits the decision to the RSU and neighbor BS. After the evaluation and formulation of the final aggregated trust degree, the BS then encrypts the trust degree using SHA2-256 [30] and RIPEMD 160 [31] with the same encryption method used by blockchain and transmits that to the neighboring base station for future use. The encrypted trust value is only shared among the base stations, whereas to reduce the computational burden, the trust value transmitted toward RSUs is not encrypted.

3.3. Recommendation-Based Trust Evaluation

The recommendation-based trust evaluation is the indirect evaluation performed when required past observations are not available. In this evaluation, the RSU acts as a central authority to broadcast requests to the neighboring RSUs to share their observations. The requested RSU has to wait for the response from the neighboring RSU after broadcasting the request. After receiving the observations, the proposed approach will apply the summation function to range them within the limit to compare it with the threshold value for decision making. The complete process of indirect recommendation-based trust evaluation is illustrated by Algorithm 2.

Algorithm 2 Recommendation-Based Trust Degree Evaluation.

```
procedure INITIAL OBSERVATIONS($n_{id}$)
    Fetch Node ID
    Broadcast request using Node ID
    Wait to receive response
procedure FORMULATION TRUST
    Trust observation computation as Equation (9)
    Trust development as Equation (10)
procedure DECISION MAKING
    If trust degree $\leq$0.7 then no trust
    If trust degree $\geq$0.8 then trustworthy
Exit
```

Another major aspect of the proposed is that it integrates blockchain that a block creates at base stations, as they always have the observations of every node. In the proposed approach, an encrypted trust degree shared by the neighboring nodes is not considered as a direct evaluation. The proposed mechanism treats it as indirect and only uses them in recommendation-based trust evaluation. Using a shared trust degree as indirect trust will enhance the accuracy of malicious node identification. The observations gathered and the summation function process performed during indirect trust evaluation is represented by Equations (9) and (10).

$$rec_{n_{id}}^{r_{id}} = rec_{n_{id}}^{td_1} + rec_{n_{id}}^{td_2} + \ldots + rec_{n_{id}}^{td_n} \tag{9}$$

$$rec_{n_{id}}^{td} = \sum_{0.0}^{n-1} \left[rec_{n_{id}}^{td_1} + rec_{n_{id}}^{td_2} + \ldots + rec_{n_{id}}^{td_n} \right] \tag{10}$$

The recommendation-based threshold for decision making is different in comparison to the direct evaluation as illustrated by Equation (11). If the trust degree is ≤ than 0.7, then nodes are considered as malicious, whereas if the trust degree ≥0.8, then nodes are listed as trustworthy.

$$\phi = \begin{cases} \text{if } rec_{n_{id}}^{td} \leq 0.7 \rightarrow NoTrust \\ \text{if } rec_{n_{id}}^{td} \geq 0.8 \rightarrow Trustworthy \end{cases} \tag{11}$$

3.4. Cluster Head Selection

After cluster formulation, it is necessary to select the head of the cluster who can lead and coordinate among the cluster members. The cluster head is responsible for communicating with all the members, along with VANET infrastructure and other cluster heads. Another significant aspect of the proposed mechanism is that it restricts the communication between different cluster members until permission is provided by the cluster head. To reduce the challenges associated with overhead, the proposed approach also selects a backup head. To date, the backup heads are used by existing approaches only when a cluster head left the cluster. Under this situation, one backup head will become a cluster head and continue performing the responsibilities. The proposed approach extends the responsibilities of the backup head; they will also operate as a load balancer and assist the cluster head as an assistant after their selection. If a cluster member needs any specific information, then it will request the backup head who is free or has the least pending jobs. The cluster members will only coordinate or broadcast information and monitor cluster members for any abnormal or malicious activity.

To implement and achieve the above-mentioned points, the proposed mechanism merges the trust degree with QoS to manage both security and quality during the selection of clusters and backup heads. The trust degree evaluation is already explained in the previous section, whereas the QoS is performed during the head's selection. The QoS parameters used by the proposed mechanism are packet delivery ratio, execution time, and mean opinion score. The complete process of QoS evaluation is represented by Algorithm 3. The computation of packet delivery ratio is illustrated by Equation (12) [32].

$$pdr_{n_{id}}^{c_{id}} = \frac{\sum(packet_{n_{id}}^{rec})}{\sum(packet_{n_{id}}^{sen})} \tag{12}$$

In Equation (12), *pdr* is the packet delivery ratio, and c_{id} is cluster ID, whereas the ratio is evaluated by the summation of packet received $(packet_{n_{id}}^{rec})$ into summation of packet send $(packet_{n_{id}}^{sen})$ by a particular node. The next step is to evaluate the execution time that shows the competence of a node to respond and execute the request received by cluster members. To evaluate the competence of a particular node, the calculation of execution time is illustrated by Equation (13) [33].

$$et_{n_{id}} = I \times CPI \times C \tag{13}$$

In Equation (13), *et* represents the execution time of a particular node (n_{id}), whereas I is the instruction count, *CPI* is the cycle per instruction, and *c* represents the clock cycle. The next process is to calculate the mean opinion score to evaluate the quality of experience observed by the cluster backup head related to the cluster head. The computations of mean opinion score are performed after the selection of cluster head, and RSUs coordinate as a central authority to manage this. In this evaluation, as illustrated by Equation (14), we use the experience related to the node to compute the mean opinion score.

$$mos_{n_{id}} = \frac{\sum_{n=1}^{N} R_n}{N} \tag{14}$$

In Equation (14), the mean opinion score is computed as the arithmetic mean which is evaluated upon the ratings provided by the backup head, whereas R_n represents the individual ratings given to the cluster head. After the evaluation of the mean opinion score, the proposed mechanism combines all the QoS parameters evaluation to formulate a single decimal value that makes it possible to merge it with the trust degree. Equation (15) represents the process of QoS parameter aggregation.

$$qos_{n_{id}}^{ab} = pdr_{n_{id}}^{c_{id}} + et_{n_{id}} + mos_{n_{id}} \tag{15}$$

In Equation (15), qos is quality of service, n_{id} is node identity, and ab shows the absolute aggregation of parameters, whereas $pdr_{n_{id}}^{c_{id}}$, $et_{n_{id}}$, and $mos_{n_{id}}$ represent the evaluation of packet delivery ratio, execution time, and mean opinion score, respectively. After formulation, the last process is to merge the QoS evaluation with the trust degree of a particular node and apply the summation function to compute the final degree of trusted quality that will be used for the decision making. The merging of trust and QoS is illustrated by Equation (16).

$$c_{n_{id}}^{tq_{ab}} = \sum_{0.0}^{1.0} \left[t_{n_{id}}^{a_{tr}} + qos_{n_{id}}^{ab} \right] \tag{16}$$

In Equation (16), c represents the candidate, n_{id} is the candidate ID, and tq_{ab} shows the absolute calculation of trust and quality. The summation is applied to the pre-computed trust degree $t_{n_{id}}^{a_{tr}}$ and $qos_{n_{id}}^{ab}$ to formulate the sole absolute degree that is utilized in Equation (17) for decision making.

$$\phi = \begin{cases} \text{if } c_{n_{id}}^{tq_{ab}} \geq 0.8 \rightarrow Head \\ \text{if } c_{n_{id}}^{tq_{ab}} \geq 0.6 \rightarrow Backup \\ \text{if } c_{n_{id}}^{tq_{ab}} \leq 0.5 \rightarrow exit \end{cases} \tag{17}$$

Equation (17) represents that if a node contains $c_{n_{id}}^{tq_{ab}}$ higher or equal to 0.8 degree, then it will be given a priority to become a cluster head. If there are multiple nodes at the same trust degree, then the approach will randomly select one as a cluster head, whereas others become the backup head according to the conditions provided by Equation (17). If there is no node containing $c_{n_{id}}^{tq_{ab}} \leq$ than 0.8, then the approach will go one step backward and consider the nodes having a higher degree greater than 0.6. If no node fulfills the criteria of having degree $\geq$ than 0.6, then the proposed approach will repeat the computation process. As mentioned, if more than one node contains a higher degree, i.e., higher than 0.8, then one will become a cluster head, whereas the rest will be considered as backup heads. The proposed approach selects at least three backup heads, and if this condition is fulfilled in the first step, then nodes having $\geq$ 0.6 will be ignored. The number of backup heads selected by the proposed is three, but if the number of nodes is less and does not fulfill the backup criteria, then the requirement to select three backup heads will be changed as per the situation.

Algorithm 3 Cluster and Backup Head Selection Process.

```
 1: procedure INITIAL OBSERVATIONS($n_{id}$)
 2:     Fetch Node ID with $t_{n_{id}}^{a_{tr}} \geq 0.6$
 3:     Rank the nodes with respect to trust degrees
 4:     if no node with $\geq 0.6$ then go to step 13
 5: procedure QOS EVALUATION
 6:     Packet delivery ratio as Equation (12)
 7:     Execution time evaluation as Equation (13)
 8:     Mean opinion score calculation as Equation (14)
 9: procedure QOS DEVELOPMENT($qos_{n_{id}}^{ab}$)
10:     Aggregation of QoS Computation as Equation (15)
11: procedure QOS AND TRUST AGGREGATION($hc_{n_{id}}^{tq_{ab}}$)
12:     Merging of QoS and Trust Degree as Equation (16)
13: procedure DECISION MAKING
14:     Selection process as illustrated by Equation (17)
15: Exit
```

3.5. Cluster Maintenance and Merging

The maintenance of clusters is a significant aspect as it is important to maintain clusters to increase the average time. The major advantage of maintenance is that it reduces computational costs and enhances the efficient utilization of resources. As elaborated in the previous section, the backup head is selected by the proposed approach. In most of the existing approaches, the purpose of these backup head selections is limited to utilization as a cluster head. The backup has no responsibilities until the time when the cluster head leaves or stops performing the required duties. In the proposed approach, the backup head is utilized to enhance the performance of a cluster. Firstly, backup heads will continuously assist the cluster head to reduce the overhead ratio. Secondly, backup heads will also monitor the performance of the cluster head and provide the observations that are utilized to calculate the mean opinion score. The proposed approach formulates the rank table after merging the QoS and Trust. This rank table will help the cluster easily select their backup head with performing computations. When the cluster head leaves the cluster, then one of the backup heads will become the cluster head and one member of the cluster will be promoted as a backup using that rank table.

The merging of clusters is a concept that is applied to the clusters that are near to each other, i.e., within the range of each other. In the proposed mechanism, the clustering merging is completed by combining the rank table. After combining the table, nodes with a higher degree will become cluster heads and backup heads. The degree of both the cluster heads may be identical, so in that case, the approach randomly selects one from them. In the case of non-merging, the rank table will be separated as per the nodes and the same process is repeated in which nodes with higher degrees will manage and coordinate the cluster. The limits within one cluster is 10 cluster members, 3 backup heads, and 1 cluster head. In the case of merging, if the cluster limit is exceeded, then nodes with lower degrees will remain neutral until the time when the cluster becomes separated. Neutral means that these nodes are not able to broadcast any information-gathering request; however, they are able to receive the information shared by the backup and cluster head.

4. Experimental Simulation and Outcomes

An extensive simulation is performed to validate the performance of the proposed mechanism with existing approaches. The comparison of the proposed mechanism is conducted between WOACNET [24], StabTrust [28], and (DL-SCHS) [22]. The simulator used in the experimental evaluation is Vehicles in Network Simulation (VEINS) [34], which is an open-source vehicular network simulator that integrates and provides the capabilities of both OMNET++ [35] and SUMO [36].

The simulation setup of the simulation is illustrated in Table 3. The selected area of simulation belongs to Islamabad Capital Territory, Pakistan, whereas the coordinates of the selected area are x-axis = 72.9754, 73.0472, and y-axis = 33.6973, 33.6685, whereas the map data are exported from an online platform OpenStreetMap [37]. The selected area is a combination of highways and narrow roads, which is needed to validate the efficiency of the proposed approach. The rest of the subsection elaborates on the different criteria of simulation and result outcomes.

Table 3. Parameters and Simulation Setup.

Parameters	Value
Simulation Time	450 (min)
Transmission Range	300 (m)
Routing Protocol	CBRD
Maximum Vehicle Speed	33 m/s
Max. Acceleration	3.5 k/m^2
Number of RSUs	11
RSUs Coverage	0.7 KM
MAC	IEEE 802.11
Mobility Model	Random-way point
Transmission Rate	8 Mbps
Size of Packet	50∼60 (Bytes)
Peak Transmission Range	300 (m)
Transport Layer Protocol	TCP/newreno
Average Inter-Vehicle Distance	4.9 (m)

4.1. *Average Cluster Head Lifetime*

The average cluster head lifetime represents the average time that is taken by a selected head to perform its responsibilities and stay as a cluster head. It is a significant aspect of clustering as the increased duration of a head lifetime provides stability that reduces the computational cost. The comparison of cluster head lifetime is performed under different scenarios, which are (i) number of nodes n vs. transmission range r and (ii) speed limit v vs. transmission range r. In the first scenario, the number of nodes increased under seven situations, whereas the minimum number of nodes is 50 and the maximum number of nodes is 250. For the transmission range in this scenario, the transmission range r increases under each situation whereas the minimum range is 100 and the maximum is 300. Figure 3 shows the comparative simulation outcome of the proposed mechanism with existing approaches.

The overall average cluster head of comparison approaches is 146.75 (sec) in the first scenario where n = 50, and r = 100. In the second scenario, the average lifetime increased to 161.75 (sec), whereas when n = 100 and r = 200, the average lifetime of all the approaches reduced to 159.5 (sec). In the next scenario, n becomes 150, r = 150, and the average time reaches 179 (sec), whereas the maximum time reached 189.5 (sec) when n = 250 and r = 300. To analyze the comparative performance of each approach individually, the WOACNET, DL-SCHS, and StabTrust overall average times of all the scenarios are 171.41 (sec), 151 (sec), and 166.43 (sec), respectively. In comparison to all the mentioned average times of existing approaches, the proposed approach has achieved an average cluster head lifetime, i.e., 187.71 (sec), which shows the efficient performance among all approaches.

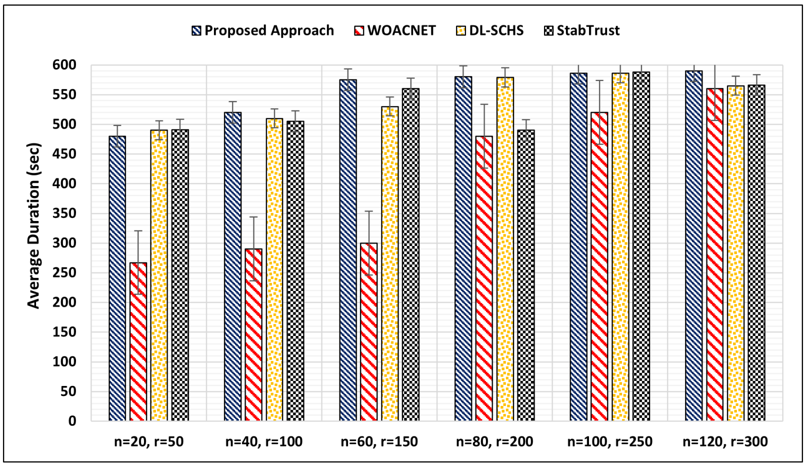

Figure 3. Comparison of Average Cluster Head Lifetime w.r.t. *n* and *r*.

The simulation analysis of cluster head lifetime is also evaluated by monitoring the performance of the approaches under a different scenario, i.e., transmission range *r* vs. speed limit of the vehicle *v*. This analysis will show the impact on the cluster head lifetime with varying speed and transmission range. The minimum transmission range is 50 and the maximum is 250, whereas the minimum speed limit of the vehicle is 30 and the maximum speed limit is set to 90. Figure 4 shows the comparative simulation outcome of the proposed approaches among existing ones. To evaluate, the overall average time of all the approaches concerning transmission range and the speed limit is 160.75 (sec) in scenario-I, 166.0 (sec) in scenario-II, 167.0 (sec) in scenario-III, 173.0 (sec) in scenario-IV, 174.5 (sec) in scenario-V, 177.75 (sec) in scenario-VI, and 181.25 (sec) in scenario-VII, respectively. To elaborate on the average performance of each approach, WOACNET maintained an average cluster lifetime of 171.41 (sec), DL-SCHS achieves a time of 151.0 (sec), whereas StabTrust reaches an average time of 166.43 (sec). In comparison to these mentioned performances, the proposed methodology has achieved an average cluster time of 187.71 (sec), which is higher than the existing approaches.

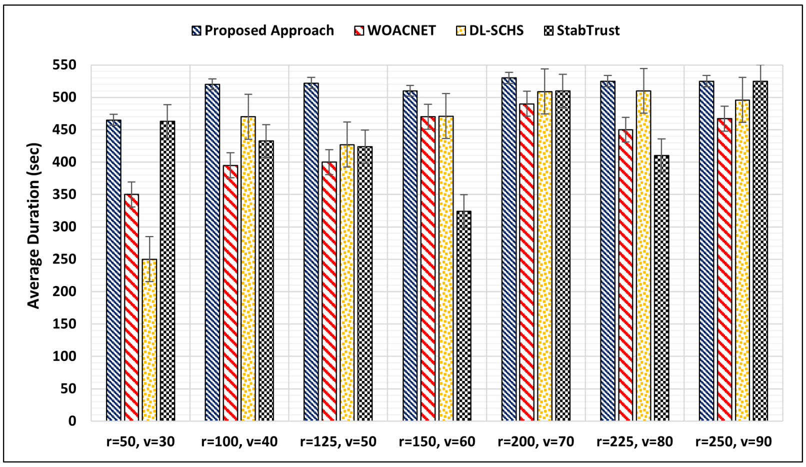

Figure 4. Comparison of Average Cluster Head Lifetime w.r.t. *r* and *v*.

If we combined the performance of each approach illustrated by Figures 3 and 4, then the average performances of these approaches are: WOANCNET has achieved an average lifetime of 170.13 (sec), DL-SCHS maintains the average cluster head lifetime of 159.13 (sec), whereas StabTrust achieved the average time of 166.86. In comparison to these approaches, the average performance of the proposed approach cluster head lifetime is 185.43 (sec) which is 15.3 (sec) higher than the approach that achieved the second-highest lifetime.

4.2. Average Cluster Lifetime

Cluster head lifetime is the primary factor, whereas cluster lifetime is the second factor to improve stability. The average cluster lifetime represents the usability or effectiveness related to backup heads. As these heads are selected to increase the cluster lifetime, the efficient utilization of these heads leads to an increase in the time duration of clusters. To evaluate the performance of the proposed approaches, two different dependent simulation scenarios are created between the varying nodes, transmission range, and the speed limit of vehicles. The first simulation scenario is between the number of nodes n vs. transmission range r with varying ranges between n = 20∼120 whereas r = 50∼300.

The average overall performance of all the approaches with varying nodes and transmission is 432.0 (sec) in scenario-I when n = 10 and r = 50, 456.25 (sec) in scenario-II when n = 40 and r = 100, 491.25 (sec) in scenario-III when n = 60 and r = 150, 532.25 (sec) in scenario-IV when n = 80 and r = 120, and 570.0 (sec) when n = 100 and r = 250. Whereas the overall average duration reaches a higher value of 570.27 (sec) when n = 120, and r = 300 as illustrated by Figure 5. The average comparative performance of each approach is: WOACNET maintained an average time of 412.0 (sec), and 536.57 (sec) is achieved by DL-SCHS, whereas StabTrust provides the maximum average lifetime of 532.12 (sec). To compare the mentioned average time, the proposed mechanism achieved an average lifetime of 560.14 (sec), which is 148.14 (sec) higher than WOACNET, 23.57 (sec) higher as compared to DL-SCHS, and 28.0 (sec) higher in comparison to StabTrust. The discussed simulation outcome shows the effective utilization of backup heads to maintain stability by providing an increased average cluster lifetime.

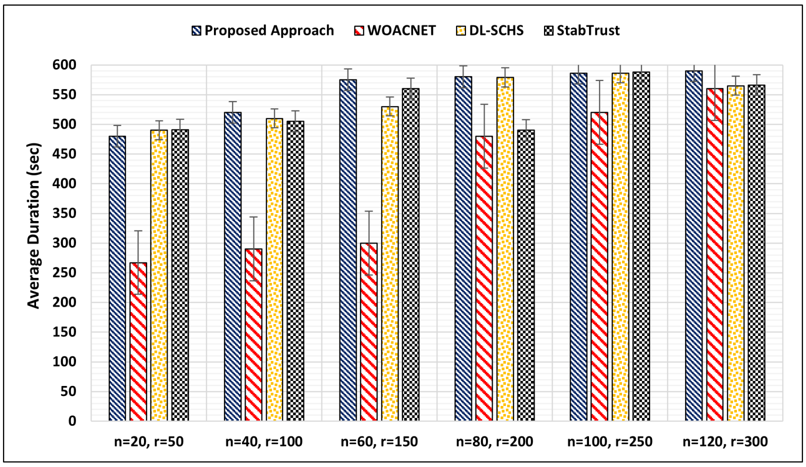

Figure 5. Comparison of Average Cluster Duration Lifetime w.r.t. n and r.

To better analyze the individual performances, it is significant to first analyze the average overall performance of all the approaches under the second simulation setup. This simulation is performed by varying the transmission range within 50∼250 and the speed limit of nodes within 30∼90, and the simulation outcome is illustrated by Figure 6. In this scenario, the overall average time achieved by approaches is 382.0 (sec) when r = 50 and v = 30, whereas the average time is increased by 77.375 (sec) in scenario-II, i.e., 459.375 (sec) when r = 100 and v = 40. Furthermore, 443.25 (sec) is achieved by the approaches in scenario-III when r = 125 and v = 50, and this time duration is increased to 443.75 (sec) in scenario-IV in which r = 150 and v = 60. In scenario-V, 509.75 (sec) duration is achieved when r = 200 and v = 70, whereas this time reduces down by 36.0 (sec) in scenario-VI, i.e., 473.75 when n = 225 and r = 90. Moreover, an increase of 29.5 (sec) is shown in scenario-VII when r = 250 and v = 90. To individually analyze comparatively the performance of these approaches, WOANCNET has achieved an average cluster lifetime of 431.72 (sec), DL-SCHS maintained an average duration of 447.75, whereas StabTrust maintained 441.21 (sec). In comparison to existing approaches, the proposed approach sustains an increased average lifetime of 71.69 (sec), i.e., 513.86 (sec). In particular, the proposed approach furnishes an increased lifetime of 82.15 (sec) in comparison with WOACNET, whereas it achieves 66.29 (sec) and 72.65 (sec) in comparison to DL-SCHS and StabTrust, respectively.

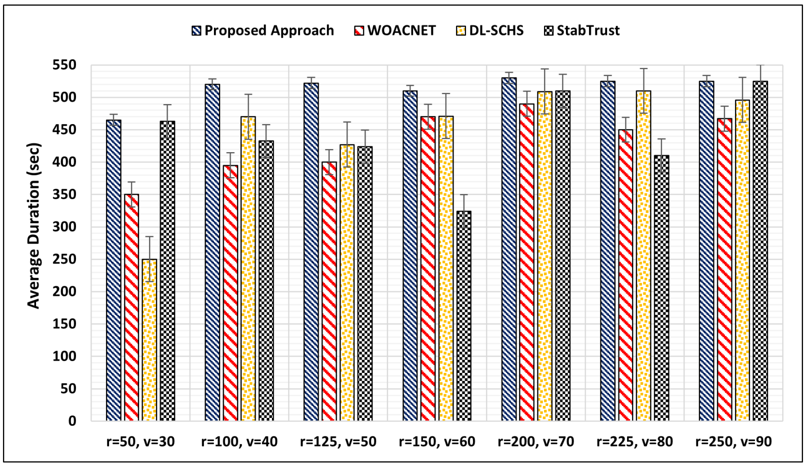

Figure 6. Comparison of Average Cluster Duration Lifetime w.r.t. r and v.

To further validate the performance of the proposed approach, we have evaluated the average performance illustrated by Figures 5 and 6, i.e., by merging n vs. r, and r vs. v. The average outcome shows that the proposed approach has achieved 537.0 (sec) in overall performance. In comparison, WOACNET achieved 421.86 (sec), 492.07 (sec) achieved by DL-SCHS, and 482.68 (sec) achieved by StabTrust. In individual comparison to each approach, the proposed mechanism furnishes an increased duration of 115.14 (sec) against WOACNET, 44.93 (sec) more in comparison to DL-SCHS, and an increased duration of 50.32 (sec) in comparison to StabTrust. The performance evaluation outcome shows that the proposed mechanism maintains more stability with an increased average cluster lifetime.

4.3. Aggregation Impact on Computations

The aggregation is a process in trust degree evaluation in which previous trust and currently evaluated trust combine to formulate a degree of trust related to a particular node. The aggregation can only be performed when the previous trust degree is available. The significance of aggregating these trust values provides the stability to trust degree. The trust degree of a particular node may vary with time, but with the aggregation, the evaluation provides a stable outcome. As mentioned in Section 3.1, the proposed methodology utilizes blockchain to encrypt the trust degree to maintain integrity. To evaluate the impact of encryption, two distinct simulation setups have been implemented in which the first is for the trust degree aggregation of trustworthy nodes and the second is for malicious nodes.

Figure 7 illustrates the simulation outcome of aggregation for the trustworthy node. The graph shows the fluctuation when the trust degree is evaluated without the aggregation process. On the other side, when the aggregation process is applied to the currently evaluated trust, the outcome shows a stable output with reduced fluctuation in the trust degree.

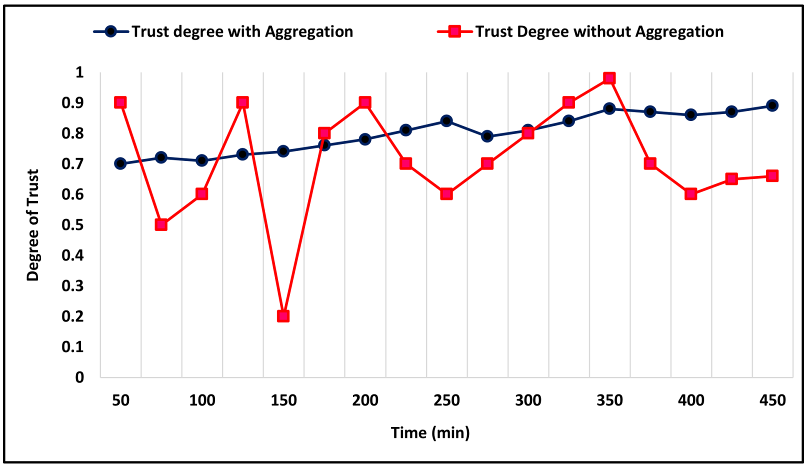

Figure 7. Comparative Analysis of Aggregation Impact on Computations of Proposed Approach Against Trustworthy Node.

The aggregation becomes more significant with the evaluation of malicious node trust degree, as this process helps to improve the detection rate. Figure 8 shows the simulation outcome of malicious node trust degree with and without the aggregation process.

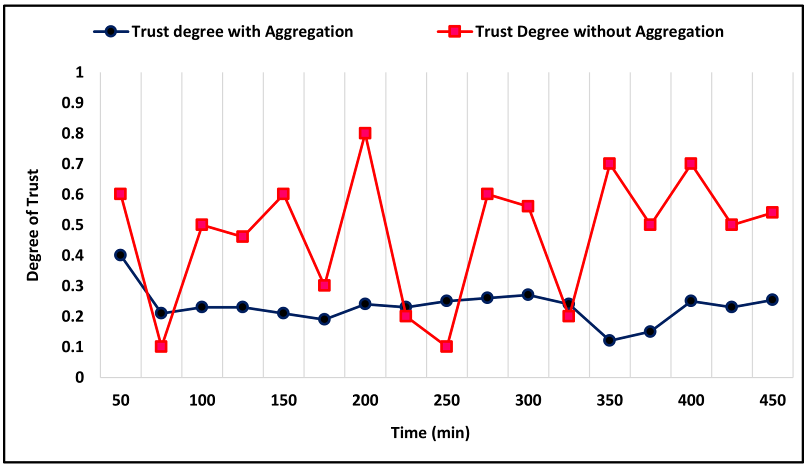

Figure 8. Comparative Analysis of Aggregation Impact on Computations of Proposed Approach Against Malicious Node.

4.4. Quality Evaluation of Cluster Head

As mentioned earlier, the proposed methodology utilizes backup heads to provide their feedback, and the mean opinion score [38] is computed to improve the quality of clusters. To further extend the responsibilities, the backup heads will also assist the cluster head to improve the efficiency that directly impacts the efficiency of the head to perform its responsibilities. To precisely evaluate the impact of the mentioned points, it is necessary to evaluate the quality improved by reducing the responsibilities of the cluster head. To evaluate quality, two scenarios are designed in which overhead [39] and throughput [40] ratios have been evaluated to formulate the level of quality. The simulation setup of this evaluation is implemented with a varying number of nodes as 30∼150, and the simulation time is 450 (min).

Figure 9 illustrates the simulation outcome of the overhead ratio. The comparison analysis among different approaches shows that the proposed approaches successfully minimize the overhead ratio. The proposed mechanism continuously maintained the low overhead ratio that shows the efficient performance of the cluster head. The overall overhead of the existing approaches is: the WOACNET average overhead is 47.1, the DL-SCHS average overhead is 45.4, whereas the StabTrust overhead ratio is 68.9. In comparison to these average ratios, the proposed approach overhead is 28.2, which is the least among all approaches. The comparative analysis of the proposed approach with existing approaches is illustrated by Figure 10. The results also validate the performance of the proposed mechanism as it maintained a low overhead ratio.

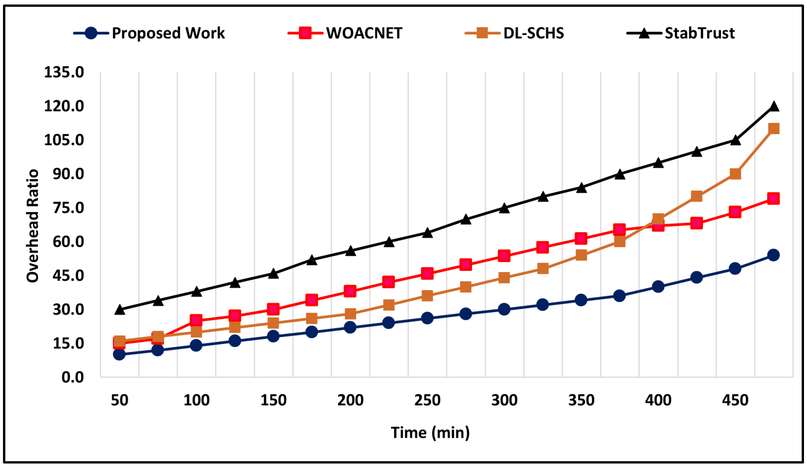

Figure 9. Average Overhead Ratio Analysis of Proposed Approach and Backup Heads Assistance.

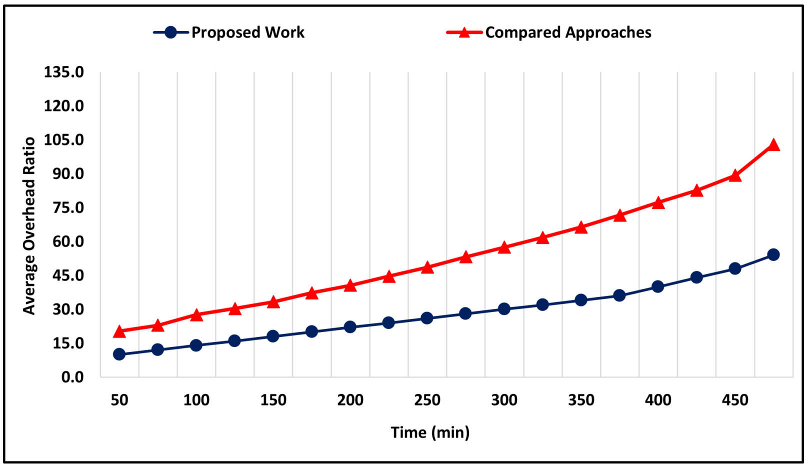

Figure 10. Average Overhead Ratio Analysis of Proposed Approach and Existing Approaches.

The second scenario of the quality analysis is the evaluation of throughput that is evaluated by monitoring the information transmitted to the cluster member and the request–response rate. Figure 11 shows the comparative simulation outcome of the throughput ratio, and the results indicate that the proposed mechanism has successfully achieved the higher throughput, whereas DL-SCHS approaches also perform significantly better in comparison to the rest of the approaches. The overall throughput ratios of the existing approaches follow: the WOACNET average throughput ratio is 541.7, the DL-SCHS average throughput is 775.0, which is higher among the existing approaches, whereas the StabTrust throughput ratio is 406.3. In comparison to these ratios, the proposed approach ratio is 796.1, which is the maximum among all approaches. For precise individual comparison, the proposed approach provides 254.1% more throughput in comparison to WOACNET, 21% more throughput in comparison to DL-SCHS, whereas it provides 389.8% more throughput in comparison to StabTrust. To further validate the performance, Figure 12 illustrates the average performance of all the existing approaches in comparison to the proposed approach. The average throughput result shows that the existing approaches achieve a ratio of 574.3, whereas the proposed approach's overall average ratio is 796.1, which is 221.8% higher.

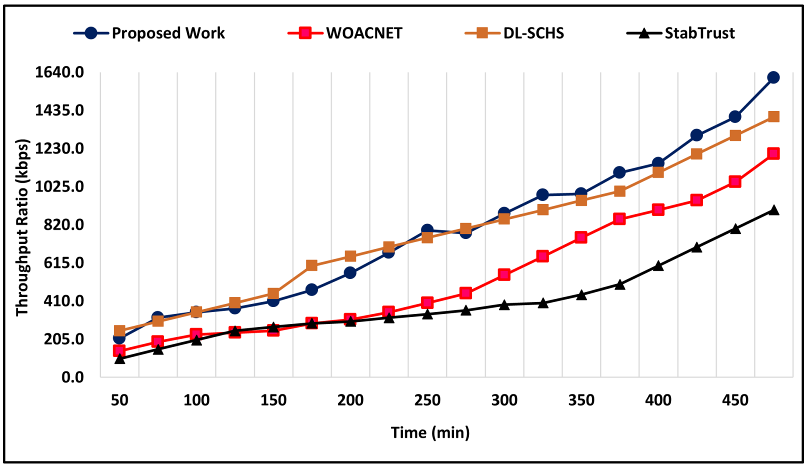

Figure 11. Average Throughput Ratio Analysis of Proposed Approach and Backup Heads Assistance.

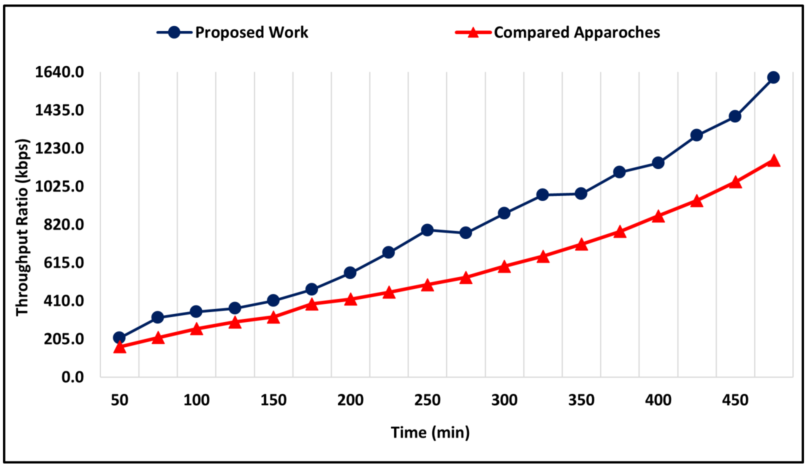

Figure 12. Average Throughput Ratio Analysis of Proposed Approach and Existing Approaches.

4.5. On–Off Attack [41]

It is the most common attack in which nodes may leave or rejoin the network to whitewash the reputation and regain the default trust degree. The situation in which nodes regain the default trust may reduce the performance of the overall VANET environment. It also provides a vulnerable source to the malicious and compromised nodes to regain default trust to affect the environment. To address this issue, the proposed mechanism uses blockchain technology to formulate an immutable ledger and encrypt the trust degrees using a unique identity of nodes. This ledger helps the proposed mechanism fetch the previous trust degree during the aggregation process to identify the nodes even if a particular node rejoins the network. The performance validation of the proposed approach is evaluated in two steps, i.e., using a varying number of nodes and evaluating it with the existing approaches.

In the first evaluation, the simulation is performed with varying nodes in the range of 40∼100, and the simulation time of each evaluation is 540 (min). Figure 13 shows the performance outcome of the proposed approach. The assigning of a lower trust degree shows that the proposed approach successfully identifies the nodes that attempt to whitewash their past reputation in the network. The overall average assigning of trust degree is 0.4, whereas when the number of nodes is 60 and 80, the proposed mechanism assigns the lowest trust degree with an average of 0.3. The assigning of the lowest trust degree represents the efficiency and accuracy of the proposed approach against on–off attack.

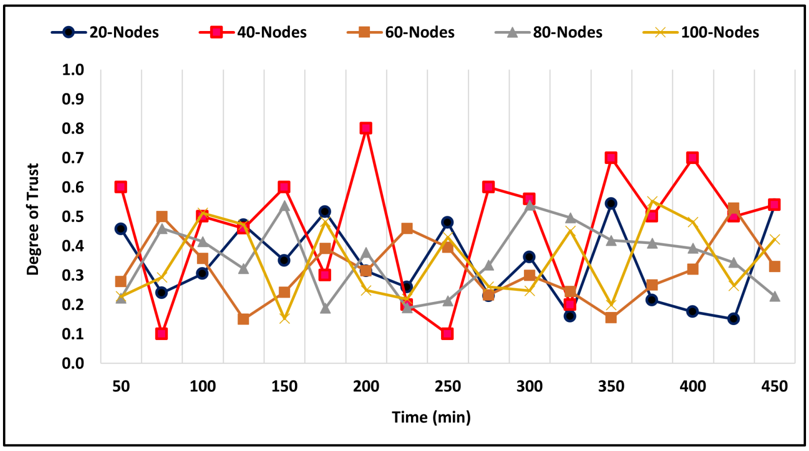

Figure 13. Performance of Proposed Approach Against On–Off Attack with Varying Nodes.

The average performance of the proposed mechanism is computed from the first simulation outcome, which is illustrated by Figure 13, and we have compared it with the performances of existing approaches against on–off attacks. Figure 14 shows the comparative simulation outcome of the proposed approach with existing approaches. As elaborated earlier, the average trust degree assigned by the proposed is 0.4, and it is also shown in Figure 14 that the average trust degree lies between 0.3 and 0.4. In comparison, the existing approaches assign a higher trust degree; however, the majority of approaches maintain effective performance but the average level of trust of these approaches is 0.4–0.6, which is higher than the proposed mechanism.

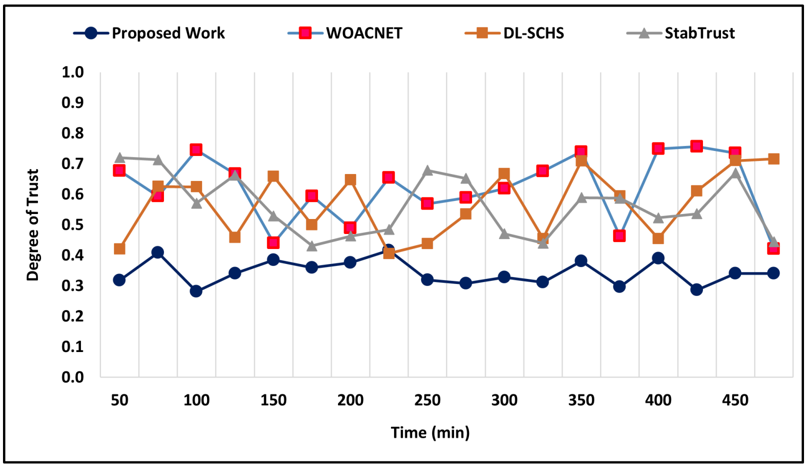

Figure 14. Comparative Analysis of Proposed Approach and Existing Approaches against On–Off Attacks.

4.6. Computational Energy Consumption

Energy consumption refers to the utilization of energy resources that are consumed by a particular approach while computing the trust degree. The efficient utilization of these resources is necessary as energy is an important factor for the successful implementation of Green VANET. The six different simulation setups with a varying number of nodes have been implemented to evaluate the computational energy consumption. Figure 15 illustrates the comparative simulation outcome of each scenario.

In the first scenario, where the number of nodes is 50, the average energy consumed by all the approaches is 138.75 (J), whereas the proposed approach consumes the least energy and StabTrust consumes a higher amount of energy to perform trust computations. In the second scenario, the number of nodes increases to 100, and overall, the energy resources consumed by the approaches are 190.75 (J), whereas StabTrust utilizes the most energy, and the least energy is consumed by DL-SCHS, which is 170 (J). In the third scenario, the number of nodes is increased to 150, whereas with a slight difference, StabTrust and WOACNET consumed 240 (J) and 230 (J), respectively. In the fourth scenario, the number of nodes is 200, whereas the average energy consumption of approaches reaches 228.75 (J). The maximum energy in this scenario is consumed by WOACNET, which is 270 (J) followed by StabTrust with 260 (J) and DL-SCHS with 240 (J). The proposed approach only consumed 145 (J), which is the least energy consumption of this scenario. In the fifth scenario, the number of nodes is 250, whereas the overall energy consumed by the approaches in this stage of simulation is 250 (J). The WOACNET approach consumed the maximum amount of energy, i.e., 310 (J), which is followed by StabTrust with 290 (J) and 260(J) by DL-SCHS. The proposed mechanism shows its effectiveness against energy consumption and only consumed 140 (J), which is 5 (J) less than the previous outcomes. In the last scenario, the number of nodes becomes 300 with the average energy consumption of this simulation setup being 283.75 (J). The resulting outcomes show that the proposed mechanism only consumed 190 (J), which is the least among other existing approaches, whereas WOACNET consumed 320 (J), which is followed by DL-SCHS and StabTrust with 310 (J) and 315 (J).

By evaluation of the average energy consumption in all the six simulation scenarios, the proposed approach consumed an average energy of 155.5 (J) followed by 227.17 (J) consumption by DL-SCHS and 240.0 (J) by WOACNET, whereas the most energy was consumed by StabTrust, which is 254.17 (J). To validate the efficient utilization of energy resources, the proposed mechanism consumed 84.5% less energy in comparison to WOACNET, 68.67% in comparison with DL-SCHS, and 98.67% less energy consumption in comparison to StabTrust. The efficient utilization of energy resources makes the proposed approach suitable for remote areas where a continuous supply of energy resources is not possible.

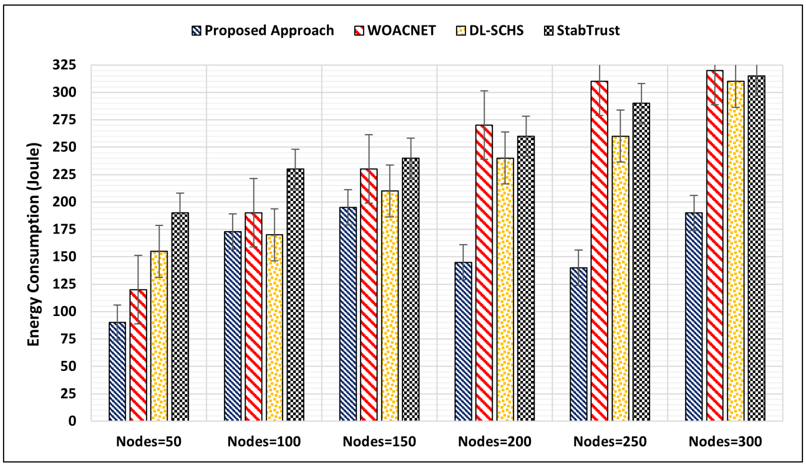

Figure 15. Comparison of Energy Consumed by Approaches During Trust Computation.

5. Conclusions

Security is significant when it comes to the successful implementation of future technologies such as IoT, VANET, etc. VANET provides communication independence to network nodes so that they can send messages to other network nodes. When the number of smart nodes increases and transmits messages, then it generates bulk communication overhead. The bulk communication may provide a chance for malicious nodes to affect the integrity and the performance of VANET. In this paper, a blockchain-based trust management mechanism is proposed that uses trust parameters to identify malicious and compromised nodes. The blockchain is integrated into the base station that encrypts the trust degrees of nodes and created an immutable ledger to maintain integrity. The encryption not only helps maintain integrity but also provides the facility to detect nodes that try to execute attacks such as on–off or whitewashing attacks. To address the challenges associated with clustering, the proposed mechanism integrates the QoS parameter during the cluster head cluster. To maintain stability, the backup heads are selected, which also assists the cluster head with improving efficiency. The proposed mechanism is a holistic solution that addresses the security, privacy, and quality challenges in parallel. The proposed mechanism is comparatively evaluated in all aspects, i.e., security attack, privacy preservation, and quality. The simulation outcome has validated the performance of the proposed mechanism and was shown to have notable improvements compared to the existing approaches. The proposed approach can be further extended to make VANET nodes and RSUs intelligent enough to detect the behavior of nodes. The intelligent capabilities bring prediction abilities that will increase the identification accuracy of malicious nodes before the trust computations.

Author Contributions: Conceptualization, K.A.A. and I.U.D.; methodology, A.A.; software, K.A.A.; validation, K.A.A., I.U.D. and A.A.; formal analysis, K.A.A.; investigation, I.U.D.; resources, A.A.; data curation, I.U.D., A.A.; writing—original draft preparation, K.A.A.; writing—review and editing, I.U.D., A.A.; visualization, A.A.; supervision, I.U.D.; project administration, A.A.; funding acquisition, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by King Saud University, Riyadh, Saudi Arabia, through Researchers Supporting Project number RSP-2022/184.

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. Awan, K.A.; Din, I.U.; Almogren, A.; Kim, B.S.; Altameem, A. vTrust: An IoT-Enabled Trust-Based Secure Wireless Energy Sharing Mechanism for Vehicular Ad Hoc Networks. *Sensors* **2021**, *21*, 7363. [CrossRef] [PubMed]
2. Saleem, Q.; Din, I.U.; Almogren, A.; Alkhalifa, I.; Khattak, H.A.; Rodrigues, J.J. Named Data Networking-Based On-Demand Secure Vehicle-To-Vehicle Communications. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 1615015. [CrossRef]
3. Malik, F.M.; Khattak, H.A.; Almogren, A.; Bouachir, O.; Din, I.U.; Altameem, A. Performance evaluation of data dissemination protocols for connected autonomous vehicles. *IEEE Access* **2020**, *8*, 126896–126906. [CrossRef]
4. Mohammad, S.A.; Rasheed, A.; Qayyum, A. VANET architectures and protocol stacks: A survey. In Proceedings of the International Workshop on Communication Technologies for Vehicles, Springer, Bordeaux, France, 16–17 November 2011; pp. 95–105.
5. Khanh, Q.V.; Hoai, N.V.; Manh, L.D.; Le, A.N.; Jeon, G. Wireless communication technologies for IoT in 5G: Vision, applications, and challenges. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 3229294. [CrossRef]
6. Hemalatha, R.; Abdul Samath, J. A Survey: Security Challenges of Vanet And Their Current Solution. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 1239–1244.
7. Zhang, Y.; Das, B.; Qiao, F. Sybil Attack Detection and Prevention in VANETs: A Survey. In Proceedings of the Future Technologies Conference, Springer, Vancouver, ON, USA, 5–6 November 2020; pp. 762–779.
8. Singh, R.; Saluja, D.; Kumar, S. Graphical Approach for V2V Connectivity Enhancement in Clustering-based VANET. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1217–1221. [CrossRef]
9. Maan, U.; Chaba, Y. Accurate Cluster Head Selection Technique for Software Defined Network in 5G VANET. *Wirel. Pers. Commun.* **2021**, *118*, 1271–1293. [CrossRef]
10. Al-Heety, O.S.; Zakaria, Z.; Ismail, M.; Shakir, M.M.; Alani, S.; Alsariera, H. A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet. *IEEE Access* **2020**, *8*, 91028–91047. [CrossRef]
11. Zhang, Z.; Deng, R.; Yau, D.K.; Cheng, P. Zero-Parameter-Information Data Integrity Attacks and Countermeasures in IoT-based Smart Grid. *IEEE Internet Things J.* **2021**, *8*, 6608–6623. [CrossRef]
12. Debnath, A.; Basumatary, H.; Dhar, M.; Bhattacharyya, B.K.; Debbarma, M.K. A Routing Technique for Enhancing the Quality of Service in Vanet. *IETE J. Res.* **2021**, 1–14. [CrossRef]
13. Wang, D.; Zhao, J.; Wang, Y. A survey on privacy protection of blockchain: The technology and application. *IEEE Access* **2020**, *8*, 108766–108781. [CrossRef]
14. Jothi, K.; Ebenezer Jeyakumar, A. Optimization and quality-of-service protocols in VANETs: a review. *Artif. Intell. Evol. Algorithms Eng. Syst.* **2015**, *324*, 275–284.
15. Awan, K.A.; Din, I.U.; Almogren, A.; Guizani, M.; Altameem, A.; Jadoon, S.U. Robusttrust–a pro-privacy robust distributed trust management mechanism for internet of things. *IEEE Access* **2019**, *7*, 62095–62106. [CrossRef]

16. Cooper, C.; Franklin, D.; Ros, M.; Safaei, F.; Abolhasan, M. A comparative survey of VANET clustering techniques. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 657–681. [CrossRef]
17. Elhoseny, M.; Shankar, K. Energy efficient optimal routing for communication in VANETs via clustering model. In *Emerging Technologies for Connected Internet of Vehicles and Intelligent Transportation System Networks*; Springer: Berlin, Germany, 2020; pp. 1–14.
18. Yogarayan, S.; Razak, S.F.A.; Azman, A.; Abdullah, M.F.A. A mini review of peer-to-peer (P2P) for vehicular communication. *Indones. J. Electr. Eng. Inform. (IJEEI)* **2021**, *9*, 185–197.
19. Sun, G.; Yu, M.; Liao, D.; Chang, V. Analytical exploration of energy savings for parked vehicles to enhance VANET connectivity. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 1749–1761. [CrossRef]
20. Hasbullah, H.; Soomro, I.A. Denial of service (DOS) attack and its possible solutions in VANET. *Int. J. Electron. Commun. Eng.* **2010**, *4*, 813–817.
21. Douligeris, C.; Mitrokotsa, A. DDoS attacks and defense mechanisms: classification and state-of-the-art. *Comput. Netw.* **2004**, *44*, 643–666. [CrossRef]
22. Saleem, M.A.; Shijie, Z.; Sarwar, M.U.; Ahmad, T.; Maqbool, A.; Shivachi, C.S.; Tariq, M. Deep learning-based dynamic stable cluster head selection in VANET. *J. Adv. Transp.* **2021**, *2021*, 9936299. [CrossRef]
23. Yu, Y.; Si, X.; Hu, C.; Zhang, J. A review of recurrent neural networks: LSTM cells and network architectures. *Neural Comput.* **2019**, *31*, 1235–1270. [CrossRef]
24. Husnain, G.; Anwar, S. An intelligent cluster optimization algorithm based on Whale Optimization Algorithm for VANETs (WOACNET). *PLoS ONE* **2021**, *16*, e0250271. [CrossRef] [PubMed]
25. Emary, E.; Yamany, W.; Hassanien, A.E.; Snasel, V. Multi-objective gray-wolf optimization for attribute reduction. *Procedia Comput. Sci.* **2015**, *65*, 623–632. [CrossRef]
26. Mirjalili, S. The ant lion optimizer. *Adv. Eng. Softw.* **2015**, *83*, 80–98. [CrossRef]
27. Nam, J.; Kim, S.M.; Min, S.G. Extended Wireless Mesh Network for VANET with Geographical Routing Protocol. In Proceedings of the 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015), Shanghai, China, 21–23 September 2015.
28. Awan, K.A.; Din, I.U.; Almogren, A.; Guizani, M.; Khan, S. StabTrust—A stable and centralized trust-based clustering mechanism for IoT enabled vehicular ad-hoc networks. *IEEE Access* **2020**, *8*, 21159–21177. [CrossRef]
29. Chen, L.; Lee, W.K.; Chang, C.C.; Choo, K.K.R.; Zhang, N. Blockchain based searchable encryption for electronic health record sharing. *Future Gener. Comput. Syst.* **2019**, *95*, 420–429. [CrossRef]
30. Chaves, R.; Kuzmanov, G.; Sousa, L.; Vassiliadis, S. Improving SHA-2 hardware implementations. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Yokohama, Japan, 10–13 October 2006; pp. 298–310.
31. Aggarwal, S.; Kumar, N. Hashes. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2021; Volume 121, pp. 83–93.
32. Tsirigos, A.; Haas, Z.J. Analysis of multipath routing-Part I: The effect on the packet delivery ratio. *IEEE Trans. Wirel. Commun.* **2004**, *3*, 138–146. [CrossRef]
33. Waheed, A.; Shah, M.A.; Khan, A.; Jeon, G. An infrastructure-assisted job scheduling and task coordination in volunteer computing-based VANET. *Complex Intell. Syst.* **2021**, 1–21. [CrossRef]
34. Sommer, C.; German, R.; Dressler, F. Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis. *IEEE Trans. Mob. Comput.* **2011**, *10*, 3–15. doi: 10.1109/TMC.2010.133. [CrossRef]
35. Varga, A. OMNeT++. In *Modeling and Tools for Network Simulation*; Springer: Berlin, Germany, 2010; pp. 35–59.
36. Lopez, P.A.; Behrisch, M.; Bieker-Walz, L.; Erdmann, J.; Flötteröd, Y.P.; Hilbrich, R.; Lücken, L.; Rummel, J.; Wagner, P.; Wießner, E. Microscopic traffic simulation using sumo. In Proceedings of the IEEE 2018 21st International Conference on Intelligent Transportation Systems (ITSC), Maui, HI, USA., 4–7 November 2018; pp. 2575–2582.
37. Open Street Map. Available online: https://www.openstreetmap.org/#map=5/30.671/69.360 (accessed on 10 November 2022)
38. Streijl, R.C.; Winkler, S.; Hands, D.S. Mean opinion score (MOS) revisited: methods and applications, limitations and alternatives. *Multimed. Syst.* **2016**, *22*, 213–227. [CrossRef]
39. Abuashour, A.; Kadoch, M. Control overhead reduction in cluster-based VANET routing protocol. In *Ad Hoc Networks*; Springer: Berlin, Germany, 2018; pp. 106–115.
40. Salvo, P.; Cuomo, F.; Baiocchi, A.; Rubin, I. Investigating VANET dissemination protocols performance under high throughput conditions. *Veh. Commun.* **2015**, *2*, 185–194. [CrossRef]
41. Zhang, J.; Zheng, K.; Zhang, D.; Yan, B. AATMS: An anti-attack trust management scheme in VANET. *IEEE Access* **2020**, *8*, 21077–21090. [CrossRef]