IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 7, 2020, accepted January 20, 2020, date of publication January 23, 2020, date of current version February 4, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2968948

StabTrust–A Stable and Centralized Trust-Based Clustering Mechanism for IoT Enabled Vehicular Ad-Hoc Networks

KAMRAN AHMAD AWAN[1], **IKRAM UD DIN**[1], **(Senior Member, IEEE),**
AHMAD ALMOGREN[2], **(Senior Member, IEEE),**
MOHSEN GUIZANI[3], **(Fellow, IEEE), AND SONIA KHAN**[4]

[1]Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[2]Chair of Cyber Security, Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
[3]Department of Computer Science and Engineering, Qatar University, Doha 2713, Qatar
[4]Department of Computer Science, COMSATS University Islamabad, Abbottabad Campus, Abbottabad 22060, Pakistan

Corresponding author: Ahmad Almogren (ahalmogren@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research, King Saud University through the Vice Deanship of Scientific Research Chairs. The authors are grateful to the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs.

ABSTRACT Vehicular Ad-hoc Network (VANET) is a modern era of dynamic information distribution among societies. VANET provides an extensive diversity of applications in various domains, such as Intelligent Transport System (ITS) and other road safety applications. VANET supports direct communications between vehicles and infrastructure. These direct communications cause bandwidth problems, high power consumption, and other similar issues. To overcome these challenges, clustering methods have been proposed to limit the communication of vehicles with the infrastructure. In clustering, vehicles are grouped together to formulate a cluster based on certain rules. Every cluster consists of a limited number of vehicles/nodes and a cluster head (CH). However, the significant challenge for clustering is to preserve the stability of clusters. Furthermore, a secure mechanism is required to recognize malicious and compromised nodes to overcome the risk of invalid information sharing. In the proposed approach, we address these challenges using components of trust. A trust-based clustering mechanism allows clusters to determine a trustworthy CH. The novel features incorporated in the proposed algorithm includes trust-based CH selection that comprises of knowledge, reputation, and experience of a node. Also, a backup head is determined by analyzing the trust of every node in a cluster. The major significance of using trust in clustering is the identification of malicious and compromised nodes. The recognition of these nodes helps to eliminate the risk of invalid information. We have also evaluated the proposed mechanism with the existing approaches and the results illustrate that the mechanism is able to provide security and improve the stability by increasing the lifetime of CHs and by decreasing the computation overhead of the CH re-selection. The StabTrust also successfully identifies malicious and compromised vehicles and provides robust security against several potential attacks.

INDEX TERMS Intelligent transport system, security, vehicular ad-hoc networks, trust-based clustering, VANET attacks.

I. INTRODUCTION

Since decades, humans lost their lives on roads in accidents [1]. The accident occurs when a driver is unable to identify the surrounding incidents. Moreover, traffic is increasing day-by-day and people get stuck in traffic jam and waste their valuable time. To address these challenges, an Intelligent Transport System (ITS) [2] has been proposed that collects the information of a particular vehicle. The collected information is further used to recognize problems on roads. The ITS is an effective system to overcome financial and social challenges of vehicles [3]. Also, it helps to control

The associate editor coordinating the review of this manuscript and approving it for publication was Lei Shu.

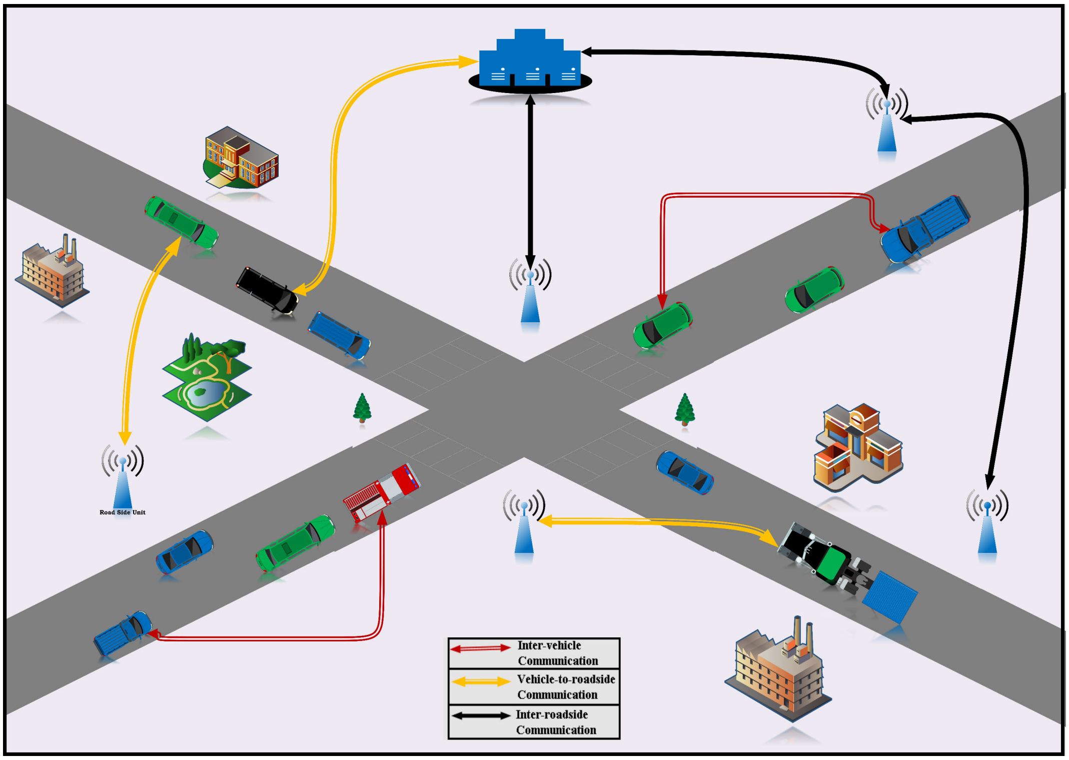
Road Side Unit
Inter-vehicle Communication
Vehicle-to-roadside Communication
Inter-roadside Communication

FIGURE 1. VANET Architecture: V2V and V2I Communications (adapted from [10]).

accidents by using pre-collected information regarding road conditions.

Vehicular Ad-hoc Network (VANET) [4] is an expansion of Mobile Ad-hoc Network (MANET) [5]. VANET supports many applications and ITS is one of them proposed to increase safety on roads. VANET consists of vehicles, Road Side Units (RSUs), and Base Stations (BS) [6]. VANET nodes have the ability to directly interact with other vehicles and infrastructure. The inter-roadside [7], inter-vehicle [8], vehicle-to-roadside communications [9], and VANET architecture are illustrated in Figure 1.

The structure of clustering consists of nodes that are divided into clusters based on their similarities [11], traffic flow [12], and other absolute rules. The composition of clusters includes cluster heads (CH), cluster gateways, and members of clusters. These approaches are further divided into several classes that include predictive clustering [13], back-bone clustering [14], MAC-based clustering [15], traditional clustering [16], Hybrid clustering [17]–[19], and secure clustering [20], [21]. The predictive clustering utilizes geographic positions and behaviors of a node to determine the formation of a cluster. In the backbone clustering, a formation of clusters is based on communications. The backbone communicates during the determination of a CH. There are many approaches proposed based on Medium Access Control (MAC) [15], [22], [23]. These MAC-based approaches use IEEE 802.11 MAC protocol [24] for the formulation of clusters [21]. A traditional clustering algorithm is sub-divided into active-based [25] and passive-based clustering [26], [27]. In active-based, a clustering mechanism continuously updates the routing record of a cluster. In passive-based [28], the formation of the cluster is performed passively. A Hybrid-based clustering approach is usually a combination of more than one mechanism. VANET supports secure clustering applications to improve safety and efficiency of a transportation network [29]. The secure authentication-based clustering (S-ABC) has been proposed, which authenticates a node to formulate a cluster and encrypt communications using an algorithm. The S-ABC approaches require a secure scheme to maintain the authentication and integrity of messages.

Despite the potential advantages, there are still numerous existing challenges for clustering [30]. These challenges include effective mechanisms for communications with least overhead that provide scalability and overcome the loss of end-to-end packet transmission [31]. Also, an efficient caching mechanism is required that can be implemented widely to cache data in the wireless networks to periodically access cached content [32]–[34]. For the Internet of Things (IoT) enabled vehicle [35], [36], a cluster based caching mechanism is required that addresses the mobility challenges of VANET nodes [37]–[41]. Multi-level clustering approaches [42], [43] have not been completely exploited yet [44]. However, an approach based on multi-level is also a challenge that uses various attributes to form a cluster. The utilization of symmetric and asymmetric key control is also a well-known challenge [18]. Besides, the efficiency and scalability along with node credibility maintenance is also a prominent challenge [45].

In this paper, a StabTrust clustering algorithm is proposed for VANETs. The trust-based clustering is a centralized approach that allows RSUs to choose a trustworthy CH for secure and authentic clustering. It provides the capability to identify malicious and compromised nodes. The proposed approach is a centralized approach in which an RSU maintains and calculates the degree of trust. If a vehicle is compromised and malicious, then the RSU will recognize it by computing the trust value. In case the vehicle is malicious and compromised, then the RSU will block it by further communicating with other vehicles and/or also from making requests to join neighboring clusters. Further, the RSU transmits the credentials and the degree of trust of a particular vehicle to the neighboring RSUs to maintain the robustness of the StabTrust. The identification of these nodes will reduce the uncertainty caused by false and invalid information. The novelty of StabTrust includes: i) A stable trust-based clustering that is accomplished by knowledge, reputation, and experience; ii) an agile identification of malicious and compromised nodes with the help of trust parameters; iii) a stable maintenance of clusters by electing a backup head based on the evaluation of a degree of trust. Furthermore, StabTrust introduces the trust propagation and aggregation mechanism that allows RSUs to share their degree of trust about a particular vehicle in addition to provide the ability to aggregate the previous trust values with the updated degree of trust. This approach utilizes several distinct trust components, i.e., knowledge, reputation, and experience that make the StabTrust robust and provide the capability to maintain resilience towards several potential attacks. Moreover, in the *experience* component of trust, the utilization of end-to-end packet delivery makes the StabTrust a step towards the green VANET because it helps the network to reduce the energy consumption. The variables used in StabTrust are calculated based on the generic mechanism of trust management proposed by [46], which consists of four essential steps, i.e., Information gathering, Trust Computation, Trust Dissemination, and Update/maintenance of the trust. The detail of subjective working of the StabTrust is elaborated in section IV.

The structure of this paper is as follows: Section II, briefly presents the current literature study of clustering approaches. Section III exhibits a detailed description of the proposed StabTrust mechanism followed by sub-sections that explain the requirements, the process of cluster formation, the components and parameters of trust, trust development, and trust threshold values among others. Section IV illustrates the performance evaluation of the proposed mechanism and Section V concludes the paper.

II. RELATED WORK

The composition of a cluster consists of vehicles containing some similar characteristics combined concurrently in a group to create a cluster. Every cluster has its unique CH that is selected on the basis of particular attributes. The CH is responsible for controlling the entire cluster and all tasks associated with communications. Several clustering approaches have been proposed for VANET.

A. SECURESTABLE-CA

A clustering algorithm for VANET is proposed to provide the security and stability on highways [47]. The proposed study is mainly focused to improve the stability and decrease the change in the vehicle status. The proposed mechanism also proposes a novel approach for the selection of CH. The primary assumption established in the proposed approach is that the vehicle has the capability of LTE [48] and 802.11p [49], and is also equipped with the GPS [50]. The formation of a cluster is initialized by a vehicle with the transmission of a beacon message. This message includes a unique ID, position, and speed of vehicle along with the acceleration and direction. When the beacon message is received, the system starts analyzing the position and detects the range of the vehicle.

The SecureStable-CA approach also utilizes the Highest-Degree [51] and Blob algorithms [52] to formulate a cluster of nearest nodes. The SecureSable-CA introduces a relative mobility metric to provide stability, improve the CH lifetime, and decrease the computation overhead of selecting a cluster. To select a CH, the proposed approach first analyzes the speed differences and acceleration of the vehicle, and applies the relative mobility metric to finalize the selection of CH. The significant contribution of the proposed scheme is the utilization of relative mobility metric that provides stability and decreases the computation overhead of selecting the cluster head over and over again.

B. HYBRID-BBCA

A hybrid backbone-based clustering algorithm (Hybrid-BBCA) [53] is proposed wherein vehicular mobility is used to formulates a cluster. This approach formulates clusters and then selects a leadership node having higher degree of connectivity. After the leadership selection, the algorithm selects a CH by examining the degree of connectivity among the leadership nodes. To select a CH, an aggregate local mobility (ALM) [54] is estimated based on diversity of its relative fluidity. A node with least ALM is elected as a CH that regulates all activities of the cluster. When a node becomes a CH, it performs its responsibilities until the heads of two clusters come in reach of each other. If two CHs are in the range of each other, one of the CHs leaves the position to merge two clusters. If the CH is away from the area of a cluster or it neglects the cluster, then the leadership will prefer to choose a new CH. If the cluster leadership has an insufficient degree of connectivity, then nodes calculate the degree of connectivity repeatedly and determine a fresh leadership along with a CH. In the Hybrid-BBCA, the stability of clusters is enhanced by the selection of leadership. The leadership selection enables the cluster to reduce the cost of computation. On the other side, the CH maintenance is declined in dense traffic conditions. Also, the acceleration of vehicles is still a challenge because with high speed, the CH endures limited time in a cluster.

C. MULTI-MBCA

A multi-metric-based clustering algorithm (Multi-MBCA) [55] is proposed, which focuses on the selection of a suitable CH. The matrices involve in the CH selection are neighboring node, node lifetime, and stability. Neighbouring node matrix is used to determine adjacent nodes. The Multi-MBCA finds the neighbors of a node based on the transmission range and makes a matrix of these nodes. The node lifetime is estimated based on the ratio of node drain rate and residual energy [56]. The node stability is calculated with respect to relative velocity [57]. The selection of CH is dependent on the stability factor of a particular node. The stability of a node is calculated based on the exchange of information among nodes. Finally, all these matrices are processed to get the normalized value. The normalized value of a matrix is further combined with the node weight factor. A node with maximum weight factor is selected as a CH.

D. MOTHFLAME-CA

A moth flame based clustering algorithm [58] is proposed for the Internet of Vehicles (IoV) [59]. The study tries to improve the lifetime that in turn augment the stability of a cluster along with the efficiency of the network. The working of MothFlame-CA is as below:

- All vehicles are moving with a random direction and speed with unique IDs.
- By utilizing the moth flame algorithm, the proposed mechanism supposes that the moths can fly in each direction, i.e., 1, 2 and 3 dimensions where the variable is vehicle location in the space.
- With the help of moths flame, the positions and directions are the main factors that help to create the cluster matrix and objective matrix to formulate a cluster.

E. PASSIVE-DCS

Another clustering algorithm, named Passive-DCS [60], is proposed for VANET that uses the passive data distribution approach to implement distributed systems. Initially, the proposed approach executes the formation of a cluster by determining neighboring nodes. The record of a neighboring node is updated when a node broadcasts a synchronization message to detect adjacent nodes. The CH is selected on the basis of position and speed. Furthermore, each node has its weight value, which is calculated by the degree difference and average speed of the node. The selection of CH depends upon the value of its weight. A node with maximum weight becomes the CH and performs its responsibilities.

F. EVOAPPROACH-CLUSTERING

A stable and optimized algorithm for clustering has been proposed that utilizes Evolutionary Game Theoretic Clustering Approach (EvoApproach-Clustering) [61]. The EvoApproach-Clustering begins by selecting a set of random nodes and applies game theory [62] to them. After that, the approach calculates the throughput of each node and applies the cost as a function. The EvoApproach-Clustering analyzes the throughput of members where a member with maximum throughput becomes the CH. If a cluster consists of minimum throughput, then every member of the cluster checks their throughput stability to find a node with maximum throughput. The Lyapunov function [63] is used for the equilibrium composition to provide better stability.

G. TRANS-CA

The transformed clustering algorithm (Trans-CA) [64] is proposed as an extension to M-SCA. The algorithm utilizes the advantages of clustering to obtain immediate delivery of emergency messages to reduce chain collisions. The Trans-CA utilizes roadside scenarios of a highway. To create a cluster, RSUs will generate a message that notifies a vehicle about entering the highway. When the vehicle enters the highway, it gets involved in the cluster creation. To select a CH, nodes share a message that includes necessary information to measure the utility function. Then, the node sends a response message back to a particular node carrying the weight of a specific node. The node owning the least weight among other nodes is elected as a CH. If a free node owns the least weight, then it selects itself as a CH and generates a message to request other nodes to join the cluster. To manage a cluster, a safety distance is employed in the maintenance phase. If one cluster enters in the area of another cluster, both CHs estimate their relative and safety distance to merge the clusters. The algorithm shows the extensive performance and reduces the cost of re-clustering. The vulnerabilities of the Trans-CA are that every node has to calculate the utility function and update other nodes to form a cluster. Every time when a node calculates and updates other nodes, it may increase the cost and create the overhead. The simulation of the Trans-CA is limited to the highway scenario, while the performance in urban roadside and effectiveness in dense traffic situations are still uncertain.

H. SCAIE CLUSTERING

The SCaIE [65] clustering algorithm is proposed that uses vehicles' behaviors to elect a CH. The algorithm selects a backup CH to enhance the stability. The vehicle periodically computes certain parameters to select the CH. The process of calculating parameters consists of a combination of different matrices. To preserve stability, means relative speed is allotted to every node. To provide stability, the algorithm determines the backup CH. If the CH does not perform its responsibilities or surrenders as a CH, then the backup CH becomes the CH. The stability is essential due to the mobility function in VANET. The strength of SCaIE is the selection of the backup CH that helps nodes to stay in connection with the head of a cluster. In VANET, a vehicle is moving at high speed which leads to mobility issues. The proposed algorithm does not specify that what will happen if the backup CH leaves before the main CH.

I. DYNAMIC-CA

The dynamic clustering algorithm (Dynamic-CA) [66] is proposed for VANET based on agents. The formation of a cluster begins by determining adjacent nodes. Nodes moving in the same direction or those which are in the range of RSUs' communications are selected as a single cluster. Next, the CH selection is executed based on the weight factor and the position of a neighboring node. The maintenance of cluster depends upon three-factor, i.e., communication range of CH, cluster members are not in the range of CH, and failure or disconnection of a link. In the Dynamic-CA, agents are used for sensing the situation of surroundings that perform certain responsibilities to achieve dynamic clustering. These agents include RSUs and vehicles which are further divided into knowledge base, information propagation, and administer agents.

J. AGGLOMERATIVE-BASED CLUSTERING

The Agglomerative approach [67] is proposed to select the CH in VANET. The parameter of quality-of-service (QoS) [68] is used to select the CH. The parameters used to formulate a cluster involves direction and speed of nodes. The size of a cluster depends upon the density of cluster. The threshold value for the density of cluster is pre-defined based on the ratio of end-to-end packet delivery. The agglomerative approach provides an efficient CH selection mechanism. However, the stability and security are still a major concern of clustering with this approach.

K. AES-CLUSTERING ALGORITHM

The AES based clustering approach (AES-CA) [46] is proposed for VANET based on density and moveability. The AES-CA applies the AES technique to encrypt and decrypt data. The formation of a cluster is based on the Euclidian formula. If nodes are in the range of Euclidian distance [69], then they become neighbors. These neighboring nodes are used in the cluster formation on the basis of density. The AES-CA utilizes the AES encryption and decryption mechanism, which consists of several steps. The AES encrypts data by the expansion of a key and then XORs the bytes. Furthermore, the AES performs different rounds in which the algorithm substitutes the bytes, shifts the rows, and mixes the columns. After that, it again adds another key and performs certain steps. In the final step, the AES generates a key that is used for the verification of a customer. This approach provides security using AES, but the stability of a cluster is still a significant challenge.

III. PROPOSED CLUSTERING APPROACH

Traditional approaches for clustering provide clusters with a mechanism utilizing certain rules and parameters. However, none of the existing clustering algorithms provides sufficient security. Furthermore, these approaches choose a CH by neglecting the security aspect. The proposed stable trust-based clustering approach (StabTrust) uses certain trust parameters to choose a CH while maintaining the trust of every node to formulate trustworthy clusters. In the StabTrust, clusters are able to recognize malicious and compromised nodes. In addition, it provides an effective mechanism to select a trustworthy CH. The RSU will estimate the trust of each node that helps to recognize and eliminate invalid information generated by malicious nodes.

The calculation of the trust parameters is performed based on the statistical model (numeric values ranging from 0.1 up to 1.0) in which an RSU observes and specifies numeric values based on the performance. The knowledge component of trust consists of integrity and cooperativeness, where the integrity parameter is co-related with the honesty component. When a node enters into the VANET environment, the RSU assigns the default trust value of 0.5 and enables a node to connect with a distinct cluster. When a node joins the cluster and interacts with others, then different neighboring nodes provide feedback to the relevant RSU based on their experience and RSUs will further refresh their trust values for future propagation and aggregation. The cooperativeness component is calculated based on the information provided by a particular node when other neighboring nodes require that information. The accurate and inaccurate information furnished by a particular node plays an important role in the calculation of cooperativeness. The calculation of reputation components is the same as discussed previously, but the trust evaluation of the experience is distinct from knowledge and reputation. The experience components of trust are estimated based on competence and end-to-end packet delivery and assessed when a node acquires a significant status in a cluster, i.e., CH or backup head. The competence parameter represents the capability of a node that how efficiently it commands a cluster or how effectively it recognizes a malicious activity and reports it to the RSU. Based on this information, the RSU will assign an absolute degree of trust, which is further used to calculate the trust by finding a summation with other trust parameters. The evaluation of subjective factors is further divided into Algorithms # 1, 2, 3 that show the calculation of parameters utilized in the proposed mechanism.

The StabTrust is a centralized clustering algorithm where the RSU is responsible for numerous computations, e.g., handling all clusters within the range, as shown in Figure 2. The RSUs execute all functions in their ranges and formulate/calculate the degree of trust to choose a CH. The trust components used in the StabTrust are knowledge, reputation, and experience. These parameters provide trustworthy clustering and enable the formation of trustworthy robust clusters to keep resilience towards compromised nodes and VANET attacks. Figure 2 represents clustering with a purple oval shape wherein the number of cluster members are indicated with black color; the backup head is depicted with a green color and node members with blue color; the CH communication with the infrastructure, i.e., V2I (Vehicle to Infrastructure Communication) is represented by red color

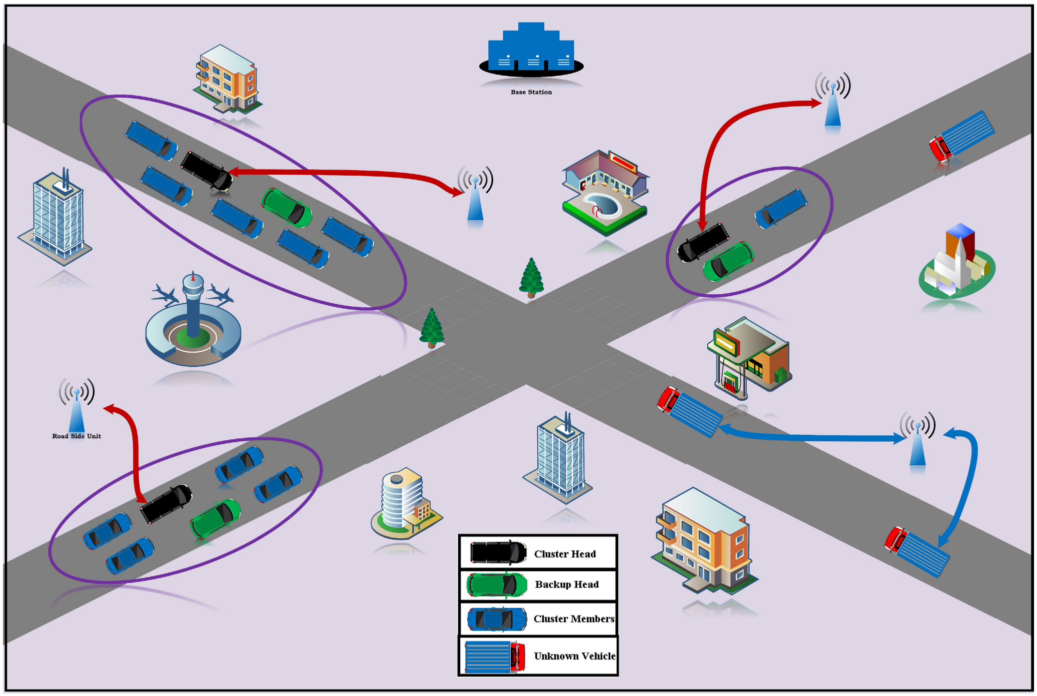

FIGURE 2. Stable trust-based clustering using RSU.

and UV communication with the infrastructure is shown by blue color, respectively.

A. CLUSTER FORMULATION

The major requirements of StabTrust to formulate a cluster are that every node must be IoT enabled so that they are able to send, receive, and store information. All VANET nodes must have a unique identity to assign the degree of trust. The RSUs will identify, calculate, and assign the estimated trust values using a unique ID.

In the formation of a cluster, an RSU acts as a central authority to formulate, coordinate, and store information of a cluster within its range. The cluster formation starts when a UV (Unknown Vehicle) joins a road and sends a cluster joining request to the nearest RSU. If the RSU finds adjacent clusters, then it sends the information of the node to an adjacent CH. The joining of a cluster is based on the direction and connectivity level. If the RSU sends the information of a node to the CH, the CH will send an invitation message to the node for joining a cluster. If the node accepts the invitation, then it will become a part of that particular cluster. The process of cluster formation is shown in Algorithm 1. If the RSU does not find any cluster, then it allows the node to start clustering. The formation of cluster depends upon the direction, connectivity level, and position of neighboring nodes. The vehicles that have the same direction and are in the range of that CH can join the cluster.

The cluster formulation begins when a new vehicle enters and transmits requests to the nearest RSU. The RSU maintains a list of all newly joining vehicles. Equation 1 shows the beginning process of generating a list of newly joining nodes.

$$Nodes = N_1, N_2, N_3, \ldots, N_n \tag{1}$$

In this equation, *Nodes* represent the table of vehicles while *N* represents a single vehicle, where 1,2,3,…,n represent the n^{th} number of new vehicles that are generating request to join the cluster.

$$Node_{new} = Node_{un} \tag{2}$$

In the beginning, RSUs interact with the new vehicle and label them with UV until that particular node joins the cluster. Equation 2 shows the labeling of new vehicle as a UV. In this equation 2 the $Node_{new}$ represents the new vehicle that enters into the network and $Node_{un}$ shows the labeling of new vehicle as an unknown vehicle.

$$Node_{un} \Longrightarrow RSU_{jreq} \tag{3}$$

After labeling new vehicle as an unknown, the UV will send the cluster a joining request through the nearest RSU. In equation 3, *Node* represents the vehicle and *un* represent an unknown vehicle request. Further, the *jreq* represents the cluster joining request of a UV.

$$RSU \Longrightarrow Node_{un}^{dir} \tag{4}$$

After receiving the joining request from the UV, the RSU will proceed further by determining the direction of the vehicle. Equation 4 elaborates the process of determining the direction where *Node* is the vehicle that transmits requests,

Algorithm 1 Cluster Formation

```
 1: procedure CLUSTER FORMATION INITIALIZATION($Node_{new}$)
 2:     $Nodes = N_1, N_2, N_3, \ldots, N_n$
 3:     $Node_{new} = Node_{un}$
 4:     $Node_{un} \Longrightarrow RSU_{jreq}, RSU \Longrightarrow Node^{dir}_{un}$
 5:     $RSU \Longrightarrow Node^{cl}_{un}$
 6:     $RSU \Longrightarrow (Node_{un} \rightarrow Clusters^{Nb})$
 7:     $RSU < notify > CH$
 8:     $CH \Longrightarrow Invites[Node_{un}]$
 9:     if $Node_{un} < invites >== Yes$ then
10:         Goto Step 14
11:     else
12:         Goto Step 04
13: procedure OBSERVATION CHECK($Node_{un}$)
14:     Required$_{observation}[k^{ic}_{node_{un}} + r^{hb}_{node_{un}} + e^{epd}_{node_{un}}]$
15:     $r^{ki}_{oc} = k^{i}_{node1\cdots nth}$
16:     $r^{kc}_{oc} = k^{c}_{node1\cdots nth}$
17:     $r^{rh}_{oc} = r^{h}_{node1\cdots nth}$
18:     $r^{rb}_{oc} = r^{b}_{node1\cdots nth}$
19:     $r^{ec}_{oc} = e^{c}_{node1\cdots nth}, r^{epd}_{oc} = e^{epd}_{node1\cdots nth}$
20:     if ($Required_{observation} = True$) then
21:         $Continue$;
22:     else
23:         $IndirectTrustEvaluation$;
24: procedure DIRECT TRUST EVALUATION($Node_{un}$)
25:     $T^{calc} \Longrightarrow \left[k^{ic}_{node_{un}}, r^{hb}_{node_{un}}, e^{cepd}_{node_{un}}\right]$
26:     $k^{i}_{node_{un}} = \sum\left[k^{i_1}_{node_{un}} + k^{i_2}_{node_{un}} + \ldots + k^{i_n}_{node_{un}}\right]$
27:     $k^{c}_{node_{un}} = \sum\left[k^{c_1}_{node_{un}} + k^{c_2}_{node_{un}} + \ldots + k^{c_n}_{node_{un}}\right]$
28:     $\sum_{0.0}^{1.0} k^{ic}_{node_{un}} = \sum\left[k^{i}_{node_{un}} + k^{c}_{node_{un}}\right]$
29:     $r^{h}_{node_{un}} = \sum\left[r^{h_1}_{node_{un}} + r^{h_2}_{node_{un}} + \ldots + r^{h_n}_{node_{un}}\right]$
30:     $r^{b}_{node_{un}} = \sum\left[r^{b_1}_{node_{un}} + r^{b_2}_{node_{un}} + \ldots + r^{b_n}_{node_{un}}\right]$
31:     $\sum_{0.0}^{1.0} r^{hb}_{node_{un}} = \sum\left[k^{h}_{node_{un}} + k^{b}_{node_{un}}\right]$
32:     $e^{c}_{node_{un}} = \sum\left[e^{c_1}_{node_{un}} + e^{c_2}_{node_{un}} + \ldots + e^{c_n}_{node_{un}}\right]$
33:     $e^{epd}_{node_{un}} = \sum\left[e^{epd_1}_{node_{un}} + e^{epd_2}_{node_{un}} + \ldots + e^{epd_n}_{node_{un}}\right]$
34:     $\sum_{0.0}^{1.0} e^{cepd}_{node_{un}} = \sum\left[k^{c}_{node_{un}} + k^{epd}_{node_{un}}\right]$
35:     $\sum_{0.0}^{1.0} T^{calc}_{node_{un}} = \sum\left[k^{ic}_{node_{un}} + r^{hb}_{node_{un}} + e^{cepd}_{node_{un}}\right]$
36: procedure TRUST FORMULATION($T^{absolute-trust}_{Node_{un}}$)
37:     RSU$\Longleftrightarrow T^{absolute-trust}_{Node_{un}}$
38:     $T^{absolute-trust}_{Node_{un}} = T^{updated}_{Node_{un}}$
39:     $\bar{x} = T^{old}_{Node_{un}} + T^{updated}_{Node_{un}}$
40: procedure DECISION PHASE($Trust^{un}_{node}$)
41:     if $T_{node_{un}} \succ Threshold$ then
42:         $accepted$
43: end
```

un represents the unknown vehicle, and dir shows the direction of the UV.

$$RSU \Longrightarrow Node^{cl}_{un} \tag{5}$$

When the RSU successfully determines the direction of the UV, the RSU determines the connectivity level of that particular node with the surrounding clusters. Equation 6 represents the process of evaluating the connectivity level in which $Node$ represent the vehicle and cl is the connectivity level of that particular vehicle.

$$RSU \Longrightarrow (Node_{un} \rightarrow Clusters^{Nb}) \tag{6}$$

After evaluating the direction and connectivity level, the RSU proceeds further to find the clusters that are suitable for that particular node. Equation 6 represents the procedure of determining the neighbouring clusters in which $Node_{un}$ is the unknown vehicle, $Clusters$ represents the available clusters in the range of RSU, and Nb is the nearby clusters to the UV.

$$RSU < notify > CH \tag{7}$$

$$CH \Longrightarrow Invites[Node_{un}] \tag{8}$$

When the RSU gathers the information of all nearby clusters, it generates a joining notification for all nearby clusters and shares the information of UV with the CH. In equation 7, the $notify$ is the notification that is transmitted by RSUs and CH is the cluster head that will receive the notification of RSUs. After receiving the request, the CH will check whether it is possible to include another vehicle or not. If it possible to include another vehicle, then the CH will transmit an invitation to that particular node. It is quite possible that more than one CH will send the invitation, in this case it depends on the vehicle to choose from them. After receiving the invitation from the CH, the node can accept and reject that invitation (see Equation 8).

$$Node_{un} < invites >== Yes \tag{9}$$

If a UV accepts the invitation of the CH, the CH will notify the RSU to evaluate the degree of trust of the particular unknown node. Equation 9 represents the acceptance of joining invitation where Yes shows the acceptance of invitation request. When the CH requests RSUs to evaluate the vehicle degree of trust, the RSU first checks that the observation required to evaluate the degree of trust is sufficient or not. If the required observation is sufficient then the RSU proceeds further to evaluate direct trust otherwise the it evaluates the indirect trust based on recommendations.

$$k^{ic}_{node_{un}} + r^{hb}_{node_{un}} + e^{cepd}_{node_{un}} \tag{10}$$

Equation 10 represents the beginning of observation check process, where RSU will check the observation of all trust parameters. These parameters are explained in Section III-B. In equation 10, $node$ is the unknown vehicle, k represents the knowledge component of trust, and i and c represent the knowledge sub-parameters, i.e., integrity and cooperativeness observations. Further, r is the reputation component of trust where h and b are the reputation sub-parameters to evaluate trust, i.e., honesty and behavior. Moreover, e represents the experience component of trust and c and epd are the experience sub-parameters to evaluate the degree of trust, i.e., competence and end-to-end packet delivery. The RSU checks the observation of all trust components to start evaluating the degree of trust. If any observation is not sufficient for the evaluation, then the RSU will evaluate trust based on recommendations.

$$r_{oc}^{ki} = k_{node_{un}}^{i} \tag{11}$$

After the initialization of observation check, the RSU checks the observation of knowledge component of trust and then its parameters. Equation 11 represents the observation check of integrity, which is a parameters of knowledge component. In equation 11, r represents the RSU, oc shows the observation check, and k and i are the knowledge and integrity, respectively. On the right side, k represents knowledge, $node$ is the vehicle, and i showa the observation check of integrity.

$$r_{oc}^{kc} = k_{node_{un}}^{c} \tag{12}$$

After the observation of integrity, the RSU checks the observation of cooperativeness parameter of knowledge. Equation 12 demonstrates the observation check of cooperativeness, which is a parameter of knowledge component. In equation 12, k and c represent the knowledge and cooperativeness, respectively. On the right side, k represents knowledge, $node$ is the vehicle and c is the observation check of cooperativeness.

$$r_{oc}^{rh} = r_{node_{un}}^{h} \tag{13}$$

When the observation check of knowledge and its parameters is completed, the RSU starts observing the reputation component of trust and its relevant parameters. Equation 13 elaborates the observation check of honesty, which is a parameter of reputation component. In this equation, r and h represent the reputation and honesty, respectively. On the right side, r represents reputation and h shows the observation check of honesty.

$$r_{oc}^{rb} = r_{node_{un}}^{b} \tag{14}$$

The RSU further checks the available observations of the second significant parameter of reputation, i.e., the behavior of vehicle. Equation 14 represents the observation check of behavior, which is a parameter of reputation component. In this equation, r and b represent the reputation and behavior, respectively. On the right side, r represents reputation of the $node$, i.e., vehicle, and b shows the observation check of behavior.

$$r_{oc}^{ec} = e_{node_{un}}^{c} \tag{15}$$

When the observation check of knowledge and reputation component of trust is completed, the RSU starts evaluating the available observations of the experience component, which is the most significant component in the StabTrust approach. Equation 15 represents the observation check of competence of vehicle, which is a parameter of experience component. In this equation, e and c are the experience and competence, respectively. On the right side, e represents experience and c is the observation check of competence.

$$r_{oc}^{eepd} = e_{node_{un}}^{epd} \tag{16}$$

At last, RSU checks the required observation of end-to-end packet delivery, which is the last parameter of the proposed mechanism. Equation 16 shows the observation check of competence of vehicle, which is a parameter of experience component. In this equation, e and epd represent the experience and end-to-end packet delivery, respectively. On the right side, c is the observation check of end-to-end packet delivery.

Finally, the RSU evaluates the available observation about a particular vehicle, which is sufficient to evaluate the degree of trust. If the required information is sufficient, the RSU starts evaluating direct trust by using the knowledge, reputation, and experience components of trust. Otherwise, the degree of trust is evaluated based on recommendations. The procedure to evaluate direct trust of a particular vehicle is illustrated in Section III-B.

B. TRUST PARAMETERS

Trust is the ability to analyze the behavior of another node whether the node is secure or malicious to communicate with. The idea of trust is essentially proposed for IoT [6] as an alternative to the traditional methods because trust evaluation involves considerable lightweight processes that will save the energy consumption and provide low-processing capabilities to nodes to secure themselves [70]. The idea of utilizing knowledge, reputation, and experience is proposed by [71], which shows the effectiveness of using these parameters. In StabTrust, the evaluation of degree of trust is based on three components of trust, i.e., knowledge, reputation, and experience. In Algorithm 1, the process of evaluation begins by the identification of a vehicle and then RSU comes to play its responsibilities by involving CHs to invite vehicles to join the cluster. When a vehicle accepts the invitation request, the CH requests the RSU to begin the evaluation of trust. The RSU initializes the process of trust evaluation by checking the required observation of that particular vehicle, as explained in Section III-A. If the required observation is available, the RSU starts evaluating direct trust, which is elaborated in this section.

$$T^{calc} \Longrightarrow \left[k_{node_{un}}^{ic}, r_{node_{un}}^{hb}, e_{node_{un}}^{cepd}\right] \tag{17}$$

Equation 17 shows the trust evaluation initialization based on numerous components of trust. The StabTrust evaluates each component one-by-one and then utilizes the summation function to formulate the absolute trust value. In equation 17,

T represents trust, where *calc* is the calculation of trust. In $k^{ic}_{node_{un}}$, k is the knowledge component of trust, $node_{un}$ shows an unknown vehicle, and *ic* represents the integrity and cooperativeness parameters of knowledge. Further, in $r^{hb}_{node_{un}}$, r represent the reputation components of trust and *hb* shows the honesty and behavior parameters of reputation. In $e^{cepd}_{node_{un}}$, e represents the experience component of trust and c and *epd* are the competence and end-to-end packet delivery, respectively.

1) KNOWLEDGE

The RSU calculates the knowledge about nodes based on integrity and cooperativeness. The integrity will allow to identify whether a node is destructive or not. In addition, it provides strength and makes secure clusters. In cooperativeness, the RSU estimates whether a node is socially cooperative or not. If the node is socially cooperative, then it will effectively coordinate the cluster. During direct trust evaluation, the first component that is evaluated is knowledge, which involves the evaluation of integrity and cooperativeness.

$$k^{i}_{node_{un}} = \sum \left[k^{i_1}_{node_{un}} + k^{i_2}_{node_{un}} + \ldots + k^{i_n}_{node_{un}} \right] \quad (18)$$

In the process of evaluating vehicles, the degree of trust begins by the evaluation of integrity parameter that involves numerous observations. Equation 18 shows the evaluation of integrity in which k represents knowledge, i is the integrity, and $i_1 + i_2 + \ldots + i_n$ shows the number of observations that the RSU has related to the integrity of a vehicle.

$$k^{c}_{node_{un}} = \sum \left[k^{c_1}_{node_{un}} + k^{c_2}_{node_{un}} + \ldots + k^{c_n}_{node_{un}} \right] \quad (19)$$

When the evaluation of integrity is completed, the RSU starts evaluating the second parameter of knowledge, i.e., cooperativeness. The cooperativeness parameter of trust shows that the vehicle is cooperative that will enhance the security of a cluster. Equation 19 represents the evaluation of cooperativeness wherein k is the knowledge, c represents cooperativeness, and $c_1 + c_2 + \ldots + c_n$ shows numerous observations that RSU utilizes to evaluate the cooperativeness of a UV.

2) REPUTATION

Reputation determines the belief of a particular node for analyzing the character of a specific vehicle. The reputation is calculated based on honesty and behavior of a node. The honesty examination indicates whether the node is honest or not. In addition, it improves the scalability of a cluster by recognizing malicious and compromised nodes. Behavior helps a node to strengthen clusters by examining the behavior of nodes towards others. After the evaluation of knowledge component and their parameters, the RSU continues evaluating trust with the evaluation of reputation component and its parameters.

$$r^{h}_{node_{un}} = \sum \left[r^{h_1}_{node_{un}} + r^{h_2}_{node_{un}} + \ldots + r^{h_n}_{node_{un}} \right] \quad (20)$$

The reputation component's evaluation begins by evaluating the honesty parameter of trust that can improve the overall scalability of cluster. Equation 30 shows the process of honesty evaluation in which r represent the reputation component of trust and $h_1+h_2+\ldots+h_n$ represents numerous observations of honesty that the RSU utilizes to evaluate the honesty of vehicles.

$$r^{b}_{node_{un}} = \sum \left[r^{b_1}_{node_{un}} + r^{b_2}_{node_{un}} + \ldots + r^{b_n}_{node_{un}} \right] \quad (21)$$

After evaluating the honesty parameter, the RSU calculates the behavior of a vehicle, which is a significant parameter because it ensures that a particular vehicle will not behave malicious after getting the higher degree of trust. Equation 21 demonstrates the process of evaluating the behavior factor of a vehicle. In this equation, r represent the reputation component of trust and $b_1 + b_2 + \ldots + b_n$ represents several observations of behavior that the RSU uses to evaluate the honesty.

3) EXPERIENCE

The trust parameter *experience* strictly belongs to the past event occurrence. The experience of one node among others is calculated based on previous experiences. The parameters to calculate experience are competence and end-to-end packet delivery. The competence is used because it determines whether the node is competent in coordinating the cluster or not. The competence property of trust is calculated based on the previous information about a particular node. The end-to-end packet delivery helps RSUs to calculate the communication cost among nodes. This property of trust provides a better clustering for the green IoT. The trust component of experience is an extra layer towards providing robust security to all clusters because it utilizes the previous experience, which means that if a vehicle performs inefficient after getting higher degree of trust, then a particular RSU will easily identify that vehicle based on the previous experience. The evaluation of experience component begins by evaluating the competence parameter of trust.

$$e^{c}_{node_{un}} = \sum \left[e^{c_1}_{node_{un}} + e^{c_2}_{node_{un}} + \ldots + e^{c_n}_{node_{un}} \right] \quad (22)$$

The evaluation of experience component starts by the evaluation of competence of a vehicle to check whether the vehicle has the capability to perform the responsibilities by joining the cluster or whether it has the capacity to take the responsibilities of CH in case it gets selected. Equation 22 represents the evaluation process of competence of a vehicle in which e represents the experience component of trust and $c_1 + c_2 + \ldots + c_n$ elaborates several observations of competence that the RSU uses durind evaluation.

$$e^{epd}_{node_{un}} = \sum \left[e^{epd_1}_{node_{un}} + e^{epd_2}_{node_{un}} + \ldots + e^{epd_n}_{node_{un}} \right] \quad (23)$$

The last parameter that the RSU evaluates during performing direct trust computation is the end-to-end packet delivery. This parameter is really significant because it helps to save the energy consumption and improve the communication along with the performance, which is an utmost important factor for green VANETs. Equation 23, represents the evaluation process of end-to-end packet delivery of a vehicle wherein e is the experience component of trust and $epd_1 + epd_2 + \ldots + epd_n$ represents the number of observations that the RSU had previously have and utilized to evaluate the end-to-end packet delivery.

C. CLUSTER FORMULATION TRUST DEVELOPMENT

The trust development allows RSUs to formulate the absolute degree of trust. After the trust component evaluation, the RSU gets six different values. The RSU starts formulating the degree of trust one-by-one starting from the knowledge component. To formulate the absolute trust value, the StabTrust mechanism utilizes the summation function. During the cluster formulation, the trust development phase first formulates the parameters of knowledge component of trust, which is represented by equation 24.

$$\sum_{0.0}^{1.0} k^{ic}_{node_{un}} = \sum \left[k^{i}_{node_{un}} + k^{c}_{node_{un}} \right] \tag{24}$$

In equation 24, $\sum_{0.0}^{1.0}$ represents the formulation of absolute trust value ranging from 0.0 to 1.0. The $k^{c}_{node_{un}}$ represents the evaluation of cooperativeness where $k^{i}_{node_{un}}$ demonstrates the trust evaluation of integrity. The trust development phase combines both the distinct value and rank them from 0.0 to 1.0, as illustrated above.

$$\sum_{0.0}^{1.0} r^{hb}_{node_{un}} = \sum \left[r^{h}_{node_{un}} + r^{b}_{node_{un}} \right] \tag{25}$$

In equation 25, $\sum_{0.0}^{1.0}$ is the formulation of absolute trust value ranging from 0.0 to 1.0. In this equation, $r^{h}_{node_{un}}$ represents the evaluation of honesty and $r^{b}_{node_{un}}$ shows the trust evaluation of behavior. The trust development phase combines both the distinct values.

$$\sum_{0.0}^{1.0} e^{cepd}_{node_{un}} = \sum \left[e^{c}_{node_{un}} + e^{epd}_{node_{un}} \right] \tag{26}$$

In equation 26, $\sum_{0.0}^{1.0}$ is the formulation of absolute trust value ranging from 0.0 to 1.0. Here, $e^{c}_{node_{un}}$ represents the evaluation of competence and $e^{epd}_{node_{un}}$ is the trust evaluation of end-to-end packet delivery. The trust development phase combines both the distinct values.

$$\sum_{0.0}^{1.0} T^{calc}_{node_{un}} = \sum \left[k^{ic}_{node_{un}} + r^{hb}_{node_{un}} + e^{cepd}_{node_{un}} \right] \tag{27}$$

After developing the trust evaluation of knowledge, reputation, and experience, the StabTrust mechanism then developes the overall trust formulation of all values. Equation 27 represents the overall trust formulation process, which formulates the absolute degree of trust to compare it with the threshold value. In this equation, $T^{calc}_{node_{un}}$ represents the trust evaluation of an unknown node where T represents the trust. On the right side, $k^{ic}_{node_{un}}$ elaborates the parameters of knowledge component, i.e., i for integrity and c for cooperativeness. Furthermore, $r^{hb}_{node_{un}}$ shows the parameters of reputation components, i.e., h shows honesty and b is used for the behavior evaluation. Moreover, $e^{cepd}_{node_{un}}$ represents the parameters of experience component, i.e., c shows the competence and epd is used for the end-to-end packet delivery. The trust development phase utlizes the summation function to rank all the values between 0.0 and 1.0, and then compares it with the threshold value. After the formulation of absolute trust value, the StabTrust continues to make a decision about joining a cluster.

After formulating the absolute trust value, the next phase is to compare it with the threshold value. If the threshold value is greater than the minimum degree of trust requirement, then vehicles are allowed to join a cluster, otherwise the CH declines to accept them as members of the cluster. The detailed description of the threshold value is illustrated in Section III-D.

D. TRUST THRESHOLD VALUES

The threshold value is the minimum value that particular vehicles require to join the cluster. When a New vehicle or UV enters the VANET environment and transmits requests for joining a cluster or start formulation clustering, the RSU will assign the initial or default degree of trust as 0.5.

In StabTrust, the minimum trust value required to join the cluster is 0.5 where the maximum trust value is 1.0 and the trust degree is ranging from 0.0 to 1.0. The degree of trust ranging from 0.0 to 0.4 is considered as no trust and a vehicle will not get permission to join the cluster. The degree of trust ranging from 0.5 to 0.7 is considered as the medium trust and in this case, vehicles containing trust degree between these are not to generate any request, message or to share any data, but can only have the permission to receive the messages or information. The trust degree ranging from 0.8 to 1.0 is considered as the superior trust and a vehicle containing the trust degree between these ranges is considered as trustworthy and it gets the priority to become the main CH or a backup CH.

As we discussed in Section III-C, after the formulation of absolute degree of trust, the StabTrust then compares the trust value with the threshold value, as presented in equation 28. In this equation, *threshold* is the minimum value required to join a cluster.

$$T^{calc}_{node_{un}} > threshold \tag{28}$$

If the trust degree of a vehicle is greater than the threshold value, then the CH accepts the vehicle as a member of cluster and it is allowed to communicate with other members of the cluster.

E. CLUSTER-HEAD SELECTION

The significance of StabTrust is that it selects the CH based on trust to achieve trustworthiness and provide a secure mechanism for clustering. These trust parameters make clusters more secure and robust. Also, it helps to easily recognize malicious and compromised nodes. Trust parameters are based on knowledge, reputation, and experience, while the indirect trust calculation is based on recommendations. These direct and indirect trust parameters are explained below and Algorithm 2 illustrates the process of a CH selection.

After the formulation of CH, the next process is to choose the CH that will coordinate and manage the cluster members. The process of selecting the CH begins by creating the list of all members associated with that particular cluster.

$$RSU \Longrightarrow Node^{n}_{ith} \tag{29}$$

The RSU is responsible to gather the information of all members of the cluster and create a list. Equation 29 shows the process of creating the list of cluster members in which the *ith* and *n* represent the total number of members currently in the cluster. After creating the list of cluster members, the RSU checks the available observations of all members to evaluate the degree of trust based on direct evaluation.

$$k^{ic}_{node_{1\cdots nth}} + r^{hb}_{node_{1\cdots nth}} + e^{cepd}_{node_{1\cdots nth}} \tag{30}$$

The RSU starts evaluation to know that whether the required observation about the $1 \ldots nth$ cluster is available or not. The process of observation check begins by the component of knowledge in which the RSU evaluates the observation of integrity and cooperativeness. In addition, the RSU checks the parameters of other components, i.e., reputation and experience. Equation 30 shows the observation check of all components of trust where *k* represents the knowledge component, *node* shows the vehicle members of cluster, and $1 \cdots nth$ demonstrates the total number of existing members. Further, *r* represents the reputation and *hb* elaborates its parameters. i.e., honesty and behavior. At last, the RSU checks the observation of experience component, which comprises the competence of vehicles and end-to-end packet delivery. The complete description of evaluating the observation of each parameter is illustrated in Section III-A. More specifically, equations 11 and 12 elucidate the observation check of integrity and cooperativeness. Equations 13 and 14 clarify the observation check of honesty and behavior, while 15 and 16 represent the observation check of competence and end-to-end packet delivery, respectively.

If the observation check of all members of clusters is sufficient enough, then the RSU starts calculating the degree of trust of each member based on direct observations. If the observation related to any specific member of cluster is not sufficient, then the RSU calculates the degree of trust based on recommendations. The process of evaluating direct trust is same as discussed earlier in Section III-B. However, the only difference here in the CH selection process is the number of nodes, which is more than one, therefore, we mention the number of nodes with $1 \ldots nth$. In Section III-B, equation 17 simplifies the beginning of direct trust evaluation and equations 18 and 19 explain the evaluation of knowledge parameters of trust. Further, equations 30 and 21 illustrate the evaluation process of honesty and behavior. At last, the RSU checks the experience components of all members of the cluster and equations 22 and 23 explicate the process of evaluating the competence and end-to-end packet delivery parameter of experience. After evaluating all components of trust, the next phase is to develop the absolute trust of all members of the clusters.

F. CLUSTER HEAD TRUST DEVELOPMENT

The development of trust means to rank the trust values according to the threshold value and formulate the absolute trust value which the StabTrust can use further for decision making. The process of trust development in StabTrust is the same as discussed in Section III-C during the formulation of cluster. However, in the CH selection, the number of vehicles is not one and during the formulation, there is only single unknown node.

$$\sum_{0.0}^{1.0} T^{calc}_{Node_{1\cdots nth}} \tag{31a}$$

$$\sum \left[k^{ic}_{node_{1\cdots nth}} + r^{hb}_{node_{1\cdots nth}} + e^{cepd}_{node_{1\cdots nth}} \right] \tag{31b}$$

Equation 31a represent the left side and 31b shows the right side of trust development process. In equation 31b, $k^{ic}_{1\cdots nth}$ exhibits the parameters of knowledge component, i.e., *i* and *c* represent the integrity and cooperativeness, respectively. Moreover, $r^{hb}_{node_{1\cdots nth}}$ explains the parameters of reputation components, i.e., *h* and *b* represent honesty and behavior, *c* shows the evaluation of competence, and *epd* represents the end-to-end packet delivery. In equation 31a, $\sum_{0.0}^{1.0}$ defines the development of absolute trust value ranging from 0.0 to 1.0. Further, $T^{calc}_{node_{1\cdots nth}}$ elaborates the evaluation of trust of cluster members where *T* represents trust, $node_{1\ldots nth}$ elucidate the total number of members, and *calc* represents the absolute calculation of trust.

After the development of trust of all nodes, the RSU compares the absolute degree of trust with the threshold value and the node with higher degree of trust gets selected as a CH, while the other top three vehicles will get selected as backup heads, which is illustrated in equation 32 that provides stability to the cluster.

$$Backup^{1\ldots3}_{Heads} = trust \succ Threshold \tag{32}$$

In equation 32, the the left side indicates the selection of at least three backup heads and any one of them will get selected as a CH when the existing head of a cluster leaves. The selection of backup heads is done by comparing the degree of trust with the threshold value and the vehicles with higher degree of trust will get selected as backup heads.

G. MAINTENANCE OF CLUSTER

The objective of maintenance of a cluster is to provide stability to clusters. The stability occurs when the CH is unable to perform the desired responsibilities or it leaves the cluster. If the stability happens again and again, then the RSU or any

Algorithm 2 Cluster Head Selection

```
procedure Cluster Head Selection($Neighbour^{nodes}$)
  RSU$\Longrightarrow$ $Node^{n}_{ith}$
  Required$_{observation}[k^{ic}_{node_{1 \cdots nth}} + r^{hb}_{node_{1 \cdots nth}} + e^{epd}_{node_{1 \cdots nth}}]$    ▷ Observation check of member vehicles
  $r^{ki}_{oc} = k^{i}_{node_{1 \cdots nth}}$    ▷ Observation check of integrity
  $r^{kc}_{oc} = k^{c}_{node_{1 \cdots nth}}$    ▷ Observation check of cooperativeness
  $r^{rh}_{oc} = r^{h}_{node_{1 \cdots nth}}$    ▷ Observation check of honesty
  $r^{rb}_{oc} = r^{b}_{node_{1 \cdots nth}}$    ▷ Observation check of behaviour
  $r^{ec}_{oc} = e^{c}_{node_{1 \cdots nth}}$    ▷ Observation check of competence
  $r^{eepd}_{oc} = e^{epd}_{node_{1 \cdots nth}}$    ▷ Observation check of end-to-end packet delivery
  if ($Required_{observation} = True$) then    ▷ Observation decision making
    $Continue$;
  else
    $IndirectTrustEvaluation$;
                                                  ▷ End of Observation Check
procedure ClTrust Evaluation($T^{calc}_{Node_{1 \cdots nth}}$)
  RSU$\Longrightarrow \left[T^{calc}_{Node_1} + T^{calc}_{Node_2} + \cdots + T^{calc}_{Node_n}\right]$    ▷ Cluster member trust evaluation
  RSU$\Longleftrightarrow T^{calc}_{Node_{1 \cdots nth}} = \left[k^{ic}_{node_{1 \cdots nth}} + r^{hb}_{node_{1 \cdots nth}} + e^{epd}_{node_{1 \cdots nth}}\right]$    ▷ Trust component evaluation
  $\mathrm{T}^{calc}_{Node_{1 \cdots nth}} \Longleftrightarrow k^{i}_{node_{1 \cdots nth}} = \left[k^{i_1}_{node_{1 \cdots nth}} + k^{i_2}_{node_{1 \cdots nth}} + \cdots + k^{i_n}_{node_{1 \cdots nth}}\right]$    ▷ Integrity Evaluation
  $\mathrm{T}^{calc}_{Node_{1 \cdots nth}} \Longleftrightarrow k^{c}_{node_{1 \cdots nth}} = \left[k^{c_1}_{node_{1 \cdots nth}} + k^{c_2}_{node_{1 \cdots nth}} + \cdots + k^{c_n}_{node_{1 \cdots nth}}\right]$    ▷ Cooperativeness evaluation
  $\sum^{1.0}_{0.0} k^{ic}_{node_{1 \cdots nth}} = \sum \left[k^{i}_{node_{1 \cdots nth}} + k^{c}_{node_{1 \cdots nth}}\right]$    ▷ Summation of knowledge component
  $\mathrm{T}^{calc}_{Node_{1 \cdots nth}} \Longleftrightarrow r^{h}_{node_{1 \cdots nth}} = \left[r^{h_1}_{node_{1 \cdots nth}} + r^{h_2}_{node_{1 \cdots nth}} + \cdots + r^{h_n}_{node_{1 \cdots nth}}\right]$    ▷ Honesty evaluation
  $\mathrm{T}^{calc}_{Node_{1 \cdots nth}} \Longleftrightarrow r^{b}_{node_{1 \cdots nth}} = \left[r^{b_1}_{node_{1 \cdots nth}} + r^{b_2}_{node_{1 \cdots nth}} + \cdots + r^{b_n}_{node_{1 \cdots nth}}\right]$    ▷ Behavior evaluation
  $\sum^{1.0}_{0.0} r^{hb}_{node_{1 \cdots nth}} = \sum \left[r^{h}_{node_{1 \cdots nth}} + r^{b}_{node_{1 \cdots nth}}\right]$    ▷ Summation of reputation trust component
  $\mathrm{T}^{calc}_{Node_{1 \cdots nth}} \Longleftrightarrow e^{c}_{node_{1 \cdots nth}} = \left[r^{c_1}_{node_{1 \cdots nth}} + r^{c_2}_{node_{1 \cdots nth}} + \cdots + r^{c_n}_{node_{1 \cdots nth}}\right]$    ▷ Competence evaluation
  $\mathrm{T}^{calc}_{Node_{1 \cdots nth}} \Longleftrightarrow e^{epd}_{node_{1 \cdots nth}} = \left[r^{epd_1}_{node_{1 \cdots nth}} + r^{epd_2}_{node_{1 \cdots nth}} + \cdots + r^{epd_n}_{node_{1 \cdots nth}}\right]$    ▷ end-to-end packet delivery evaluation
  $\sum^{1.0}_{0.0} e^{cepd}_{node_{1 \cdots nth}} = \sum \left[e^{c}_{node_{1 \cdots nth}} + e^{epd}_{node_{1 \cdots nth}}\right]$    ▷ Summation of experience component
  $\sum^{1.0}_{0.0} T^{calc}_{Node_{1 \cdots nth}} = \sum \left[k^{ic}_{node_{1 \cdots nth}} + r^{hb}_{node_{1 \cdots nth}} + e^{cepd}_{node_{1 \cdots nth}}\right]$    ▷ Absolute trust formulation
                                                  ▷ End of Trust Variable Calculations
procedure Absolute Trust Formulation($\mathrm{T}^{absolute-trust}_{Node_{1 \cdots nth}}$)    ▷ Assigning absolute trust to members
  RSU$\Longleftrightarrow T^{absolute-trust}_{Node_{1 \cdots nth}}$
  $\mathrm{T}^{absolute-trust}_{Node_{1 \cdots nth}} = T^{updated}_{Node_{1 \cdots nth}}$
  $\bar{x} = T^{old}_{Node_{1 \cdots nth}} + T^{updated}_{Node_{1 \cdots nth}}$    ▷ Finding mean value
                                                  ▷ End of Finding the Absolute Degree of Trust
procedure Decision Phase($cluster^{head}$)
  if $\mathrm{T}_{node_{1 \cdots nth}} \succ Threshold$ then    ▷ Trust value comparison of each node
    Select $nth_{node}$ as Cluster Head    ▷ Selection of cluster head
    $decline$
  RSU Backup$^{1 \cdots 3}_{Heads} = trust \succ Threshold$    ▷ Selection of backup cluster head
exit
```

other centralized authority has to choose a new CH that raises the cost of maintenance. To minimize this issue, StabTrust chooses backup heads and assigns rankings to each head for CH when the existing CH resigns. If the merging of two processes occurs, then the RSU would also merge the backup head. After the selection of CH, the RSU selects the backup heads, as explained in equation 32. The RSU prioritises these backup heads, thus, it is easy to choose the new CH when the old CH leaves the cluster. The selection of several backup heads makes the proposed mechanism suitable for the green VANET because it reduces the energy consumption.

H. CLUSTER MERGING AND NON-MERGING

Clusters merging begins when two nodes acting as CHs enter within a communication range of each other. Both CHs send a merging request to the RSU for the execution of merging process. The threshold value of nodes to join a single cluster is predefined. The RSU will not merge clusters if the merging of two clusters exceeds the threshold value. The threshold value of cluster merging in StabTrust is 10 except for the CH and backup CH. In case the merging of two clusters exceeds this value, the CHs are not allowed to merge the clusters and both the CHs will continue to perform their responsibilities. If the merging of two clusters does not exceed the threshold value of cluster merging, then two CHs will merge both the clusters and request the RSU to select a new CH. The RSU then calculates the degree of trust of both CHs and choose the new CH with higher degree of trust. The RSU may also merge the backup heads and choose the minimum three backup heads from both clusters. In a case, during the process of merging, if any vehicle travels outside the communication range of the current CH, then that vehicle will transmit a request to the most imminent RSU to join the neighboring cluster. If there is no neighboring cluster available, then the RSU will enable the node to begin the formulation of the cluster.

I. RECOMMENDATIONS

This property of trust is used in a situation if the RSU does not have any information to calculate the trust of a particular node. Algorithm 3 elaborates the procedure of trust evaluation based on recommendations. If a node is participating in a cluster formation or CH selection and the RSU does not have any past information about that particular node, then it requests the adjacent RSUs to get recommendations. The RSU uses these recommendations to carry out the trust calculations of nodes.

$$RSU_{1\rightarrow nth} \tag{33}$$

Algorithm 3 Recommendation-Based Trust Evaluation

```
1: procedure RECOMMENDATION GATHERING(RSU$_{recommendations}$)
2:     RSU$\Longrightarrow$ Node$^{n}_{i_{th}}$
3:     $\sum_{0.0}^{1.0} r^{RSU}_{i\rightarrow n_{th}} = r^{rsu_1}_{1\rightarrow n_{th}} + r^{rsu_2}_{1\rightarrow n_{th}} + r^{rsu_n}_{1\rightarrow n_{th}}$
4: procedure ABSOLUTE TRUST FORMULATION($T^{absolute-trust}_{Node1\cdots n_{th}}$)
5:     RSU$\Longleftrightarrow$ $T^{absolute-trust}_{Node}$
6:     $\mathrm{T}^{absolute-trust}_{Node1\cdots nth} = T^{updated}_{Node_{1\ldots N_{th}}}$
7:     $\overline{x} = T^{old}_{Node_{1\ldots nth}} + T^{updated}_{Node_{1\ldots n_{th}}}$
8: procedure DECISION PHASE($Trust$)
9:     if $T_{node_{1\ldots nth}} \succ Threshold$ then
10:        Assign Trust-value to particular $n^{th}{}_{node}$
11:        $Block\ n^{t}h_{node}\ communication$
```

Equation 33 signifies the recommendation gathering request from neighbouring RSUs and the neighbouring RSUs would provide their degree of trust related to a specific vehicle, and finally calculates trust based on these recommendations.

$$\sum_{0.0}^{1.0} r^{RSU}_{i\rightarrow n_{th}} = r^{rsu_1}_{1\rightarrow n_{th}} + r^{rsu_2}_{1\rightarrow n_{th}} + r^{rsu_n}_{1\rightarrow n_{th}} \tag{34}$$

Equation 34 denotes the recommendations received from the neighboring RSU. The RSU ranks these recommendations and evaluates the absolute trust value from all recommendations received by using the summation function. In this equation, $\sum_{0.0}^{1.0}$ reveals the formulation of absolute trust value that is ranging from 0.0 to 1.0. Further, r represents the recommendations, $r_{1\rightarrow n_{th}}$ shows several distinct recommendations received from a particular RSU, and rsu_1, rsu_2, and rsu_{nth} are RSUs that respond back and transmit their recommendations towards the requested RSU. The RSU then compares the absolute recommendation values with the threshold value to decide whether a vehicle is allowed to join the cluster or not.

J. TRUST PROPAGATION AND AGGREGATION

The StabTrust is a continuous process and RSUs calculate the degree of trust continuously to attain accuracy. The trust propagation and aggregation components are used to combine the past values of trust with the updated ones. The StabTrust is proposed for the IoT enabled vehicles where the past trust values about a node is stored in a specifically dedicated storage with a unique identity of a vehicle. RSUs are allowed to fetch that previous trust and perform propagation and aggregation. The StabTrust is based on quantitative data and ranges of trust value are between 0 and 1. In these ranges, 1 shows the highest degree of trust, 0.5 signifies trust ignorance, and 0 is the lowest degree of trust. The past values and the updated ones are combined mutually to formulate an absolute degree of trust to choose a trustworthy CH.

$$\overline{x} = T^{old}_{Node_{1\ldots nth}} + T^{updated}_{Node_{1\ldots nth}} \tag{35}$$

Equation 35 shows the aggregation of old trust value with the updated one and finds the mean value from them to identify the absolute aggregate of both values. In this equation, $\overline{x}$ denotes the finding of mean values, t indicates the trust, *node* specifies a particular vehicle, $1 \cdots nth$ exhibits the number of old observation, while *old* and *updated* represent the old and new trust computations.

IV. PERFORMANCE EVALUATION

To evaluate the performance of the proposed mechanism with that of the existing protocol, we have utilized OMNet++ Simulator [72]. The proposed scheme is evaluated against several significant challenges, i.e., average cluster member and CH duration, stability convergence, control overhead by speed and vehicle, throughput, and energy consumption among several potential attacks. The comparison of StabTrust is done with SecureStable-CA [47] and MothFlame-CA [58]. After the valuation of the components of trust, the StabTrust ranks them between 0.0 to 1.0, as elaborated in Section III-D.

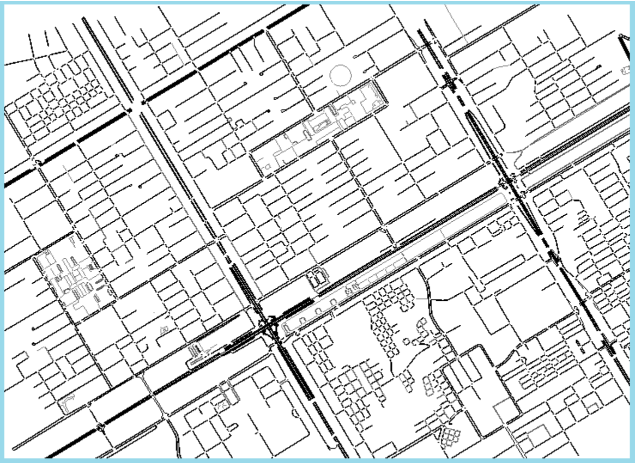

FIGURE 3. Map of Islamabad Capital Territory in SUMO.

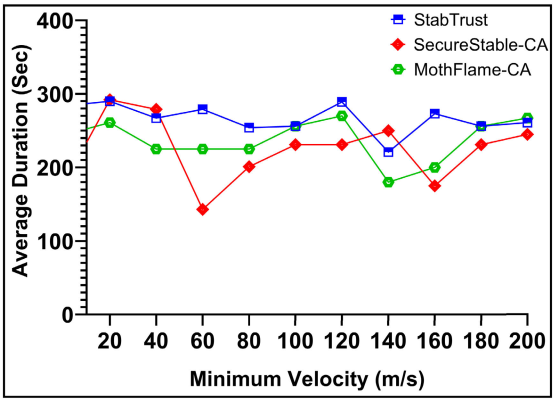

FIGURE 4. Average Cluster Duration.

We have integrated the simulation in Urban Mobility (SUMO) [73] to evaluate the real word environment. In simulations, we have deployed 60 nodes randomly in the area of 200 m^2 and the medium access protocol is IEEE 802.11 [74]- a standard protocol with a transmission range of 8 Mbps. The rest of simulation parameters are illustrated in Table 1. All the simulations were performed with numerous distinct vehicles that enter a particular area of Islamabad capital territory from different entry points and meet other vehicles, as shown in Figure 3.

A. CLUSTER HEAD LIFETIME

The CH lifetime represents the period of a node to become and leaves as a CH. When one CH leaves to perform as a CH, the approach selects the new CH from the available nodes. The time in which a cluster node becomes a CH and leaves the cluster is called the cluster head lifetime. The cluster head's lifetime is a very significant aspect to examine the stability of the mechanism because if a cluster head remains the head of a particular cluster for a long interval of time, then it will enhance the stability as well as reduce the computational cost caused by performing numerous computations to select CHs after a short span of time.

TABLE 1. Simulation parameters.

Parameters	Value
Area of network	200 m^2
Number of nodes	60
Simulation time	150 s
Transmission range	350 m
Routing protocol	CBRD
MAC	IEEE 802.11
Mobility model	Random way point
Transmission rate	8 Mbps
Size of packet	50 Bytes
Position of RSU	x = 400, y = 400
Average speed of vehicle	35 m/sec, 45m /sec, 55 m/sec

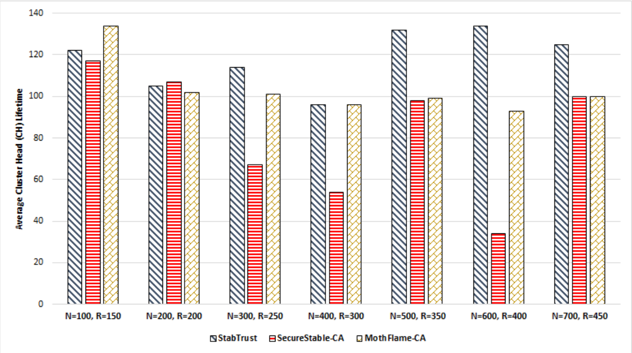

FIGURE 5. Average Cluster Head Lifetime with N & R.

During the evaluation of the average head lifetime, we have first analyzed the performance of the proposed mechanism by using two variables, i.e., number of nodes n and transmission range r. These two variables are really significant to evaluate the stability of the proposed approach. When n=100 and r=150, the performance of the MothFlame-CA is significantly higher among others. The performance of the SecureStable-CA mechanism is analyzed as effective when n and r both are equal to 200. The performance of the StabTrust will become better as the number of nodes and the transmission range increase. At n=600 and r=400, the cluster head lifetime of the proposed scheme touches the higher duration of 130 (sec) as compared to other approaches. Figure 5 depicts the simulation results of the proposed mechanism at 7 different comparative scenarios.

In VANETs, every node moving at a distinct speed and implementing the stability to the clusters is remarkably challenging for the cluster approaches. To validate the stability effectiveness of the StabTrust, we have chosen the variables of speed limit v and transmission range r. We have examined

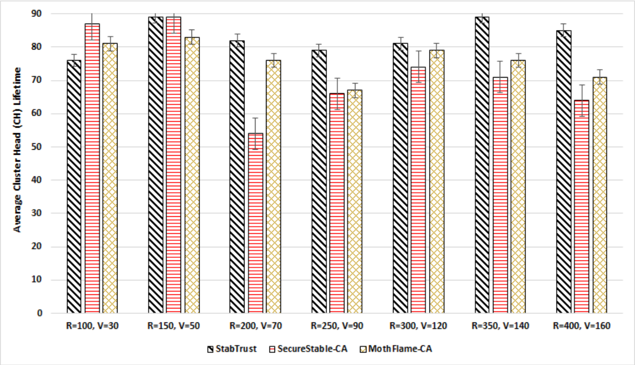

FIGURE 6. Average Cluster Head Lifetime with R & V.

the stability of the cluster at diverse values of *v* and *r*, and the results explicate that the performance of the proposed mechanism functions effectively and provides adequate stability needed for the VANET environment. Figure 6 represents the simulation results and shows the performance of StabTrust in which at r=150, v=50 the proposed mechanism reaches the higher stability level of 89 (sec). Similarly, at r=350, v=140, and r=400, v=160, the StabTrust repeatedly performs effectively and attains the stability level of 89 and 86, respectively.

B. AVERAGE CLUSTER LIFETIME

The cluster lifetime describes the duration of a particular cluster that is maintained for a specific period. The average cluster lifetime is the total average time of all clusters. The cluster lifetime is a significant aspect of VANET because formulating a cluster again and again increases the resources of energy consumption that is not suitable for green VANET [75]–[77]. Further, if the average cluster head lifetime decreases, it will directly affect the stability and may compromise the security of VANETs and all participating nodes that share and communicate with neighboring nodes.

Figure 4 exhibits the average cluster lifetime of the total cluster formulated during the simulation. The transmission range of the nodes is 200 m, the transmission rate is 8 Mbps, where the average number of nodes is 123, and the average speed of vehicles varies between 45-55 m/sec. To validate the stability of the proposed mechanism, it is significant to evaluate the average cluster head duration along with the average cluster head lifetime. During the evaluation of the average cluster duration, we have analyzed that the performance of StabTrust is significantly stable but at a minimum velocity of 140 (m/s), its performance reduces with the lowest cluster continuation of 210 (sec) and at the same time, the SecureStable-CA average cluster time reaches 250 (sec). The higher cluster duration of the proposed mechanism can be analyzed at a minimum velocity of 120 (m/s) and the duration of the cluster at a particular time is 300 (sec), which is more eminent cluster duration time in the whole evaluation of cluster duration.

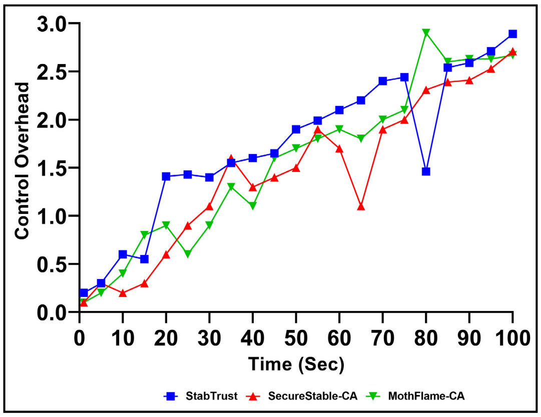

FIGURE 7. Control Overhead.

C. CONTROL OVERHEAD

The control overhead refers to the ratio of packets transmitted to the cumulative numbers of packets delivered or distributed among nodes/vehicles. The parameter of control overhead illustrates the performance of the clustering approaches. Figure 7 represents the comparative performance of clustering approaches between the number of nodes and control overhead.

The simulation among clustering approaches explicates that the performance of StabTrust is significantly more reliable and constantly improved as compared to other approaches. Figure 7 clearly shows that the StabTrust performance to control the overhead is really stable. The packet size that is transmitted from one node to another or any node that broadcasts a message is shown vertically. Moreover, the minimum size of the packet is 0.0 at time interval 0, which gradually increases with the passage of time. In comparison to other approaches, StabTrust successfully transmits the incoming traffic from the nodes and handles the overhead at time interval 18 (minute). In addition, at a time interval of 80 minutes, the proposed scheme loses the packet data shown in the figure by declining line. In comparison, MothFlame-CA encounters difficulties in delivering a packet and restraining the overhead, as shown in the figure by continuously fluctuating lines. The SeccureStable-CA performance, at the beginning from time interval 10 up to 34 (minutes), is remarkably efficient, but it is inadequate to control the overhead within the time interim of 60 up to 71 (minutes).

D. AVERAGE THROUGHPUT

Throughput is another performance measurement that refers to the rate of total packets transmitted successfully in a particular time frame. The comparative outcome of the simulation is illustrated in Figure 8, which shows that the performance of StabTrust is much more reliable as compared to SecureStable-CA and MothFlame-CA, as it achieves higher value of average throughput.

In contrast, to evaluate the control overhead, the evaluation of throughput is also a significant perspective to analyze the

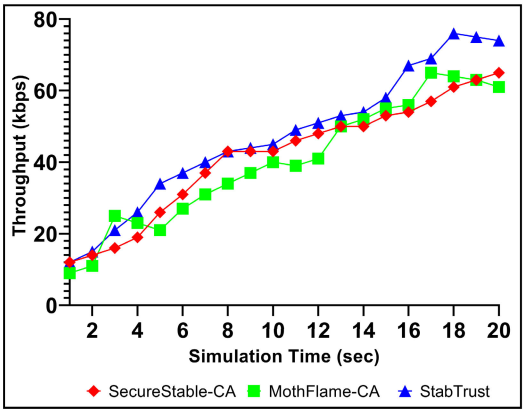

FIGURE 8. Throughput.

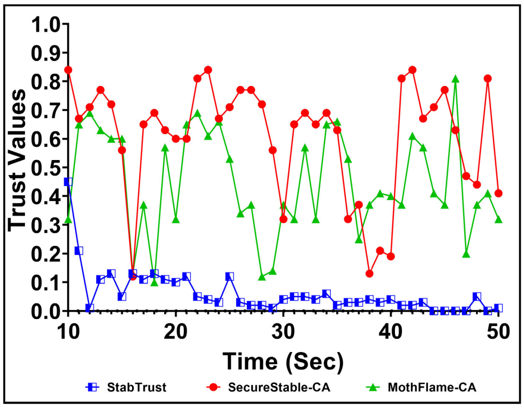

FIGURE 9. StabTrust Performance Against Sybil Attack.

efficiency of delivering transmitted packets to destinations. The simulation result in Figure 8 exhibits the continuous raising graph of StabTrust that validates its effective performance. In addition, it also indicates the packet delivery performance of SecureStable-CA, which is remarkable. The simulation result of MothFlame-CA represents fluctuation between the time internal 2 up to 9 (minutes), which shows that the mechanism faces difficulty while delivering a transmitted packet.

E. SYBIL ATTACK DETECTION

StableTrust is proposed to maintain the required security in VANET that has been significantly ignored over a decade and the focus of research stays towards the performance of the clustering. Security in VANET is a significant aspect and to achieve the maximum performance, it is essential to provide robust security. To validate the performance of StabTrust. it is evaluated against one of the most severe Sybil attacks. This attack is considered as the most notable security intimidation to VANETs in which a particular malicious node acts as a multiple identities to obtain specific advantage and generate misleading information among nodes that can cause serious quandaries.

The performance of StabTrust is evaluated, which is depicted in Figure 9. The parameters used in the StabTrust to provide security have performed really competently and successfully detected the Sybil attack. Furthermore, the malicious node is unable to gain higher trust values as compare to other approaches in which malicious nodes gain higher degree of trust over a specific period of time.

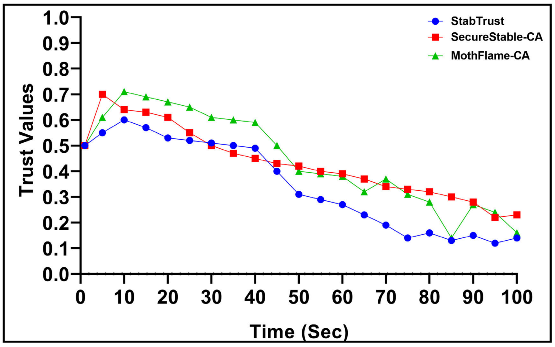

FIGURE 10. StabTrust Performance Against Warm-hole Attack Detection.

F. WARM-HOLE ATTACK

It is a novel security intimidation to vehicles in VANETs where a pair of nodes formulates a tunnel to transmit information packets from one end of the network to the other. The worm-hole attack can interrupt operations of multicast and broadcast messages. The experimental setup to simulate the Worm-hole attack are as follows: The total number of nodes = 40, transmission range = 350 m, transmission rate = 8 Mbps, default trust values = 0.5, and the size of packet is between 45-50 bytes.

The performance of StabTrust is evaluated against the security threat attack, where Figure 10 shows the performance of the proposed approach. The StabTrust successfully detects the Worm-hole attack and estimates the lower degree of trust that can help other nodes to easily identify malicious nodes with a lower degree of trust.

G. ENERGY CONSUMPTION

The efficient utilization of energy resources is vital for green VANETs. The reason behind implementing the stability is to diminish energy consumption and further to reduce the computational cost. To accomplish both factors, the evaluation of energy consumption is quite important. The vital amount of energy is consumed when nodes transmit data packets during V2V or V2I communications.

Figure 11 illustrates an average amount of energy consumed by the clustering mechanisms along with the proposed mechanism during the whole simulations. The energy consumption is represented by the energy unit, Joule. The simulation result clearly shows that the energy consumption of StabTrust in comparison with others is more limited and the SecureStable-CA consumes the highest amount of energy. The less consumption of energy represents that the StabTrust mechanism is suitable for those nodes that have less capability of storing energy and do not have enough ability to perform the computation over and over again.

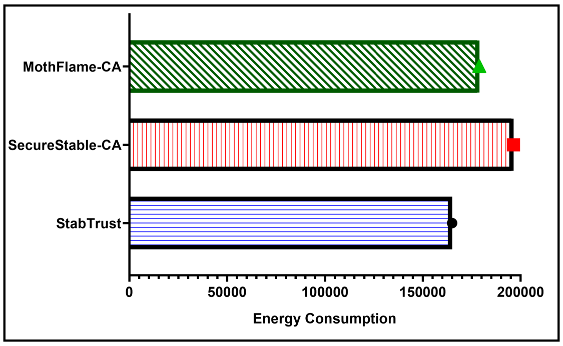

FIGURE 11. Energy Consumption Comparison of StabTrust.

V. CONCLUSION

Several clustering algorithms for VANETs have been proposed, where all of them have some advantages and disadvantages. The majority of existing approaches focuses only on the formation of clusters and selection of CH by neglecting security aspects. Furthermore, the current clustering approaches use parameters like relative velocity, ALM, Euclidean distance, weight factor, etc. to choose a CH. These parameters may allow clusters to select a CH but do not provide a secure mechanism to formulate trustworthy clusters. None of the existing clustering approaches addresses this issue and lacks in formulating trustworthy clusters. In this paper, a StabTrust clustering approach is proposed to address these security issues. StabTrust provides an approach to formulate trustworthy and secure clusters. In addition, it utilizes knowledge, reputation, and experience components of trust to maintain the degree of trust among nodes of a cluster. Also, a node with supreme trust is elected as a CH, which enhances trust among nodes to believe on an information generated by a node. The experimental simulations validate the performance of StabTrust against significant security threats while maintaining lower energy consumption. Moreover, the proposed work is further enhanced by using certain rules along with the trust parameters to propose a hybrid clustering approach that combines QoS and trust-based security at the same time. In addition, it is significant to evaluate the stability of the proposed work by comparing the cluster member with the cluster size. The StabTrust can also be further extended to develop bidirectional clustering approach for VANETs.

ACKNOWLEDGMENT

The authors would like to thank the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs.

REFERENCES

[1] T. Anjuman, S. Hasanat-E-Rabbi, C. K. A. Siddiqui, and M. M. Hoque, "Road traffic accident: A leading cause of the global burden of public health injuries and fatalities," in *Proc. Int. Conf. Mech. Eng.*, Dhaka, Bangladesh, Dec. 2020, pp. 29–31.

[2] M. A. Javed, S. Zeadally, and E. B. Hamida, "Data analytics for cooperative intelligent transport systems," *Veh. Commun.*, vol. 15, pp. 63–72, Jan. 2019.

[3] A. Papagiannakis, I. Baraklianos, and A. Spyridonidou, "Urban travel behaviour and household income in times of economic crisis: Challenges and perspectives for sustainable mobility," *Transp. Policy*, vol. 65, pp. 51–60, Jul. 2018.

[4] H. Hartenstein and K. Laberteaux, *VANET: Vehicular Applications and Inter-Networking Technologies*, vol. 1. Hoboken, NJ, USA: Wiley, 2010.

[5] S. A. A. Shah, E. Ahmed, F. Xia, A. Karim, M. Shiraz, and R. M. Noor, "Adaptive beaconing approaches for vehicular ad hoc networks: A survey," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1263–1277, Jun. 2018.

[6] I. Din, B.-S. Kim, S. Hassan, M. Guizani, M. Atiquzzaman, and J. Rodrigues, "Information-centric network-based vehicular communications: Overview and research opportunities," *Sensors*, vol. 18, no. 11, p. 3957, Nov. 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/11/3957

[7] M. R. Jabbarpour, A. Marefat, A. Jalooli, and H. Zarrabi, "Could-based vehicular networks: A taxonomy, survey, and conceptual hybrid architecture," *Wireless Netw.*, vol. 25, no. 1, pp. 335–354, 2019.

[8] H. Peng, L. Liang, X. Shen, and G. Y. Li, "Vehicular communications: A network layer perspective," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1064–1078, Feb. 2019.

[9] T. Mamatha, "An efficient cluster based routing protocol using hybrid FCM-Q LEACH for vehicular ad hoc networks," *Int. J. Appl. Eng. Res.*, vol. 14, no. 7, pp. 1604–1612, 2019.

[10] P. Bedi and V. Jindal, "Use of big data technology in vehicular ad-hoc networks," in *Proc. Int. Conf. Adv. Comput., Commun. Inf. (ICACCI)*, Sep. 2014, pp. 1677–1683.

[11] A. Rahim, X. Kong, F. Xia, Z. Ning, N. Ullah, J. Wang, and S. K. Das, "Vehicular social networks: A survey," *Pervasive Mobile Comput.*, vol. 43, pp. 96–113, Jan. 2018.

[12] L. Liu, C. Chen, T. Qiu, M. Zhang, S. Li, and B. Zhou, "A data dissemination scheme based on clustering and probabilistic broadcasting in VANETs," *Veh. Commun.*, vol. 13, pp. 78–88, Jul. 2018.

[13] B. Ženko, S. Džeroski, and J. Struyf, "Learning predictive clustering rules," in *Proc. Int. Workshop Knowl. Discovery Inductive Databases*. Berlin, Germany: Springer-Verlag, 2005, pp. 234–250.

[14] P. K. Sahu, E. H.-K. Wu, J. Sahoo, and M. Gerla, "BAHG: Back-bone-assisted hop greedy routing for VANET's city environments," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 199–213, Mar. 2013.

[15] H. Su and X. Zhang, "Clustering-based multichannel MAC protocols for QoS provisionings over vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3309–3323, Nov. 2007.

[16] L. Zhang, W.-D. Zhou, and L. Jiao, "Kernel clustering algorithm," *Chin. J. Comput.-Chin. Ed.*, vol. 25, no. 6, pp. 587–590, 2002.

[17] M. A. Wong, "A hybrid clustering method for identifying high-density clusters," *J. Amer. Stat. Assoc.*, vol. 77, no. 380, pp. 841–847, Dec. 1982.

[18] R. S. Bali, N. Kumar, and J. J. Rodrigues, "Clustering in vehicular ad hoc networks: Taxonomy, challenges and solutions," *Veh. Commun.*, vol. 1, no. 3, pp. 134–152, Jul. 2014.

[19] M. Al-Rabayah and R. Malaney, "A new scalable hybrid routing protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2625–2635, Jul. 2012.

[20] L. Bononi and C. Tacconi, "Intrusion detection for secure clustering and routing in mobile multi-hop wireless networks," *Int. J. Inf. Secur.*, vol. 6, no. 6, pp. 379–392, Oct. 2007.

[21] J. Raodawande, S. Silakari, and A. Deen, "A Survey of all existing clustering protocols in VANETS but main emphasis of survey laid on currently using protocol ie TCDGP," *Int. J. Comput. Appl.*, vol. 118, no. 6, pp. 22–31, May 2015.

[22] L. Bononi, M. Di Felice, L. Donatiello, D. Blasi, V. Cacace, L. Casone, and S. Rotolo, "Design and performance evaluation of cross layered MAC and clustering solutions for wireless ad hoc networks," *Perform. Eval.*, vol. 63, no. 11, pp. 1051–1073, Nov. 2006.

[23] M. S. Almalag, S. Olariu, and M. C. Weigle, "TDMA cluster-based MAC for VANETs (TC-MAC)," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2012, pp. 1–6.

[24] T. Salman and R. Jain, "A survey of protocols and standards for Internet of Things," 2019, *arXiv:1903.11549*. [Online]. Available: https://arxiv.org/abs/1903.11549

[25] M. Aissa, A. Belghith, and B. Bouhdid, "Cluster connectivity assurance metrics in vehicular ad hoc networks," *Procedia Comput. Sci.*, vol. 52, pp. 294–301, Jan. 2015.

[26] T. Jin Kwon, M. Gerla, V. Varma, M. Barton, and T. Hsing, "Efficient flooding with passive clustering—An overhead-free selective forward mechanism for ad hoc/sensor networks," *Proc. IEEE*, vol. 91, no. 8, pp. 1210–1220, Aug. 2003.

[27] S.-S. Wang and Y.-S. Lin, "PassCAR: A passive clustering aided routing protocol for vehicular ad hoc networks," *Comput. Commun.*, vol. 36, no. 2, pp. 170–179, Jan. 2013.

[28] D. Zhang, H. Ge, T. Zhang, Y.-Y. Cui, X. Liu, and G. Mao, "New multi-hop clustering algorithm for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 4, pp. 1517–1530, Apr. 2019.

[29] B. Jan, H. Farman, M. Khan, M. Talha, and I. U. Din, "Designing a smart transportation system: An Internet of Things and big data approach," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 73–79, Aug. 2019.

[30] O. Senouci, Z. Aliouat, and S. Harous, "A review of routing protocols in Internet of vehicles and their challenges," *Sensor Rev.*, vol. 39, no. 1, pp. 58–70, Jan. 2019.

[31] S. Allani, T. Yeferny, and R. Chbeir, "A scalable data dissemination protocol based on vehicles trajectories analysis," *Ad Hoc Netw.*, vol. 71, pp. 31–44, Mar. 2018.

[32] I. U. Din, S. Hassan, M. K. Khan, M. Guizani, O. Ghazali, and A. Habbal, "Caching in information-centric networking: Strategies, challenges, and future research directions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1443–1474, 2nd Quart., 2018.

[33] S. H. Bouk, S. H. Ahmed, and D. Kim, "Vehicular content centric network (VCCN): A survey and research challenges," in *Proc. 30th Annu. ACM Symp. Appl. Comput. (SAC)*, 2015, pp. 695–700.

[34] I. U. Din, S. Hassan, A. Almogren, F. Ayub, and M. Guizani, "PUC: Packet update caching for energy efficient IoT-based information-centric networking," *Future Gener. Comput. Syst.*, to be published.

[35] W. Ejaz, M. A. Azam, S. Saadat, F. Iqbal, and A. Hanan, "Unmanned aerial vehicles enabled IoT platform for disaster management," *Energies*, vol. 12, no. 14, p. 2706, Jul. 2019.

[36] I. Ud Din, M. Guizani, S. Hassan, B.-S. Kim, M. K. Khan, M. Atiquzzaman, and S. H. Ahmed, "The Internet of Things: A review of enabled technologies and future challenges," *IEEE Access*, vol. 7, pp. 7606–7640, 2019.

[37] M. K. Hasan and O. Sarker, "Routing protocol selection for intelligent transport system (ITS) of VANET in high mobility areas of Bangladesh," in *Proc. Int. Joint Conf. Comput. Intell.* Singapore: Springer, 2020, pp. 123–135.

[38] I. Ud Din, M. Guizani, B.-S. Kim, S. Hassan, and M. K. Khan, "Trust management techniques for the Internet of Things: A survey," *IEEE Access*, vol. 7, pp. 29763–29787, 2019.

[39] H. A. Khattak, H. Farman, B. Jan, and I. U. Din, "Toward integrating vehicular clouds with IoT for smart city services," *IEEE Netw.*, vol. 33, no. 2, pp. 65–71, Mar. 2019.

[40] I. U. Din, H. Asmat, and M. Guizani, "A review of information centric network-based Internet of Things: Communication architectures, design issues, and research opportunities," *Multimedia Tools Appl.*, vol. 78, no. 21, pp. 30241–30256, Nov. 2019.

[41] S. Hassan, I. U. Din, A. Habbal, and N. H. Zakaria, "A popularity based caching strategy for the future Internet," in *Proc. ITU Kaleidoscope, ICTs Sustain. World (ITU WT)*, Nov. 2016, pp. 1–8.

[42] R. Regin and T. Menakadevi, "Dynamic clustering mechanism to avoid congestion control in vehicular ad hoc networks based on node density," *Wireless Pers. Commun.*, vol. 107, no. 4, pp. 1911–1931, Aug. 2019.

[43] A. Manzoor, M. A. Shah, H. A. Khattak, I. U. Din, and M. K. Khan, "Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges," *Int. J. Commun. Syst.*, p. e4033, Jun. 2019.

[44] H. Khattak, Z. Ameer, U. Din, and M. Khan, "Cross-layer design and optimization techniques in wireless multimedia sensor networks for smart cities," *Comput. Sci. Inf. Syst.*, vol. 16, no. 1, pp. 1–17, 2019.

[45] I. U. Din, M. Guizani, J. J. Rodrigues, S. Hassan, and V. V. Korotaev, "Machine learning in the Internet of Things: Designed techniques for smart cities," *Future Gener. Comput. Syst.*, vol. 100, pp. 826–843, Nov. 2019.

[46] A. Sharma, E. S. Pilli, A. P. Mazumdar, and M. C. Govil, "A framework to manage trust in Internet of Things," in *Proc. Int. Conf. Emerg. Trends Commun. Technol. (ETCT)*, Nov. 2016, pp. 1–5.

[47] X. Cheng and B. Huang, "A center-based secure and stable clustering algorithm for VANETs on highways," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–10, Jan. 2019.

[48] A. Singla, S. R. Hussain, O. Chowdhury, E. Bertino, and N. Li, "Protecting the 4G and 5G cellular paging protocols against security and privacy attacks," *Proc. Privacy Enhancing Technol.*, vol. 2020, no. 1, pp. 126–142, Jan. 2020.

[49] D. Shukla, V. Kumar, and A. Prakash, "Performance evaluation of IEEE 802.11p physical layer for efficient vehicular communication," in *Advances in VLSI, Communication, and Signal Processing*. Singapore: Springer, 2020, pp. 51–60.

[50] M. S. Grewal, A. P. Andrews, and C. G. Bartone, *Global Navigation Satellite Systems, Inertial Navigation, and Integration*. Hoboken, NJ, USA: Wiley, 2020.

[51] Z. Wang, J. Yu, L. Wang, and Z. Wang, "Improved clustering algorithm based on AOW clustering algorithm," in *Proc. 7th Int. Conf. Inf., Commun. Netw. (ICICN)*, Apr. 2019, pp. 163–166.

[52] J. Wu, F. Huang, W. Hu, W. He, B. Tu, L. Guo, X. Ou, and G. Zhang, "Study of multiple moving targets' detection in fisheye video based on the moving blob model," *Multimedia Tools Appl.*, vol. 78, no. 1, pp. 877–896, Jan. 2019.

[53] J. P. Singh and R. S. Bali, "A hybrid backbone based clustering algorithm for vehicular ad-hoc networks," *Procedia Comput. Sci.*, vol. 46, pp. 1005–1013, Jan. 2015.

[54] M. S. Talib, A. Hassan, Z. A. Abas, and M. Faeq, "Clustering in VANETs perspective: Concepts, topology and applications," *Studies*, vol. 28, no. 8, pp. 471–484, 2019.

[55] J. Prakash, R. Kumar, S. Kumar, and J. P. Saini, "A multi-metric-based algorithm for cluster head selection in multi-hop ad hoc network," in *Next-Generation Networks*. Singapore: Springer, 2018, pp. 513–524.

[56] Q. Ren and G. Yao, "An energy-efficient cluster head selection scheme for energy-harvesting wireless sensor networks," *Sensors*, vol. 20, no. 1, p. 187, Dec. 2019.

[57] D. Kosmanos, A. Argyriou, and L. Maglaras, "Estimating the relative speed of RF Jammers in VANETs," *Secur. Commun. Netw.*, vol. 2019, pp. 1–18, Nov. 2019.

[58] M. F. Khan, F. Aadil, M. Maqsood, S. H. R. Bukhari, M. Hussain, and Y. Nam, "Moth flame clustering algorithm for Internet of Vehicle (MFCA-IoV)," *IEEE Access*, vol. 7, pp. 11613–11629, 2019.

[59] Z. Ning, J. Huang, X. Wang, J. J. P. C. Rodrigues, and L. Guo, "Mobile edge computing-enabled Internet of vehicles: Toward energy-efficient scheduling," *IEEE Netw.*, vol. 33, no. 5, pp. 198–205, Sep. 2019.

[60] A. Touil and F. Ghadi, "Efficient dissemination based on passive approach and dynamic clustering for VANET," *Procedia Comput. Sci.*, vol. 127, pp. 369–378, Jan. 2018.

[61] A. A. Khan, M. Abolhasan, and W. Ni, "An evolutionary game theoretic approach for stable and optimized clustering in VANETs," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4501–4513, May 2018.

[62] J. Antoniou, "Using game theory to characterize trade-offs between cloud providers and service providers for health monitoring services," in *Game Theory, the Internet of Things and 5G Networks*. Cham, Switzerland: Springer, 2020, pp. 85–106.

[63] S. Liu, D. Liberzon, and V. Zharnitsky, "Almost Lyapunov functions for nonlinear systems," *Automatica*, vol. 113, Mar. 2020, Art. no. 108758.

[64] A. A. Hashim, A. R. M. Shariff, and S. I. Fadilah, "The modified safe clustering algorithm for vehicular ad hoc networks," in *Proc. IEEE 15th Student Conf. Res. Develop. (SCOReD)*, Dec. 2017, pp. 263–268.

[65] G. V. Rossi, Z. Fan, W. H. Chin, and K. K. Leung, "Stable clustering for ad-hoc vehicle networking," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6.

[66] P. Hubballi, A. V. Sutagundar, and R. Belagali, "Agent based dynamic clustering for hybrid VANET (ADCHV)," in *Proc. IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT)*, May 2016, pp. 382–386.

[67] P. Bhosale and A. Vidhate, "An agglomerative approach to elect the cluster head in VANET," in *Proc. Int. Conf. Signal Process., Commun., Power Embedded Syst. (SCOPES)*, Oct. 2016, pp. 1340–1344.

[68] K. Shankar, M. Ilayaraja, K. S. Kumar, and E. Perumal, "Mobility and QoS analysis in VANET using NMP with salp optimization models," in *Emerging Technologies for Connected Internet of Vehicles and Intelligent Transportation System Networks*. Cham, Switzerland: Springer, 2020, pp. 15–26.

[69] A. B. Lubis and M. Lubis, "Optimization of distance formula in k-nearest neighbor method," *Bull. Elect. Eng. Inform.*, vol. 9, no. 1, pp. 326–338, 2020.

[70] K. A. Awan, I. U. Din, M. Zareei, M. Talha, M. Guizani, and S. U. Jadoon, "HoliTrust—A holistic cross-domain trust management mechanism for service-centric Internet of Things," *IEEE Access*, vol. 7, pp. 52191–52201, 2019.

[71] K. A. Awan, I. U. Din, A. Almogren, M. Guizani, A. Altameem, and S. U. Jadoon, "RobustTrust—A pro-privacy robust distributed trust management mechanism for Internet of Things," *IEEE Access*, vol. 7, pp. 62095–62106, 2019.

[72] A. Varga, "A practical introduction to the OMNeT++ simulation framework," in *Recent Advances in Network Simulation*. Cham, Switzerland: Springer, 2019, pp. 3–51.

[73] M. Behrisch and M. Weber, *Simulating Urban Traffic Scenarios*. Berlin, Germany: Springer, 2018.

[74] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," in *Proc. IEEE Veh. Technol. Conf. (VTC-Spring)*, May 2008, pp. 2036–2040.

[75] H. A. Khattak, S. U. Islam, I. U. Din, and M. Guizani, "Integrating fog computing with VANETs: A consumer perspective," *IEEE Commun. Stand. Mag.*, vol. 3, no. 1, pp. 19–25, Mar. 2019.

[76] K. Haseeb, N. Islam, A. Almogren, I. Ud Din, H. N. Almajed, and N. Guizani, "Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs," *IEEE Access*, vol. 7, pp. 79980–79988, 2019.

[77] A. Toor, S. U. Islam, N. Sohail, A. Akhunzada, J. Boudjadar, H. A. Khattak, I. U. Din, and J. J. Rodrigues, "Energy and performance aware fog computing: A case of DVFS and green renewable energy," *Future Gener. Comput. Syst.*, vol. 101, pp. 1112–1121, Dec. 2019.

KAMRAN AHMAD AWAN received the bachelor's degree in computer science from the Department of Information Technology, The University of Haripur, in 2015, where he is currently pursuing the M.S. degree in computer science with the Department of Information Technology. His current interest includes information security, graphical-user authentication, vehicular ad-hoc network, and Internet of Things with a particular emphasis on its trust management mechanisms.

IKRAM UD DIN (Senior Member, IEEE) received the M.Sc. degree in computer science and the M.S. degree in computer networking from the Department of Computer Science, University of Peshawar, Pakistan, and the Ph.D. degree in computer science from the School of Computing, Universiti Utara Malaysia (UUM). He served as the IEEE UUM Student Branch Professional Chair. He is currently working as a Lecturer with the Department of Information Technology, The University of Haripur, Pakistan. He has ten years of teaching and research experience in different universities/organizations. His current research interests include resource management and traffic control in wired and wireless networks, vehicular communications, mobility and cache management in information-centric networking, and the Internet of Things.

AHMAD ALMOGREN (Senior Member, IEEE) received the Ph.D. degree in computer science from Southern Methodist University, Dallas, TX, USA, in 2002. He worked as the Vice Dean of the Development and Quality with the College of Computer and Information Sciences (CCIS). He also served as the Dean of the College of Computer and Information Sciences and the Head of the Academic Accreditation Council at AlYamamah University. He is currently a Professor with the Computer Science Department, CCIS, King Saud University (KSU), Riyadh, Saudi Arabia, where he is also the Director of the Cyber Security Chair. His research areas of interest include mobile-pervasive computing and cyber security. He served as the General Chair for the IEEE Smart World Symposium and a Technical Program Committee Member in numerous international conferences/workshops, such as IEEE CCNC, ACM BodyNets, and the IEEE HPCC.

MOHSEN GUIZANI (Fellow, IEEE) received the B.S. (Hons.) and M.S. degrees in electrical engineering and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He served as the Associate Vice President of Graduate Studies, Qatar University, Qatar, the University of Idaho, Western Michigan University, and the University of West Florida. He is currently a Professor with the CSE Department, Qatar University. He is the author of nine books and more than 700 publications in refereed journals and conferences. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grids. He received the 2017 IEEE Communications Society Recognition Award for his contribution to outstanding research in *Wireless Communications*. He is also the Editor-in-Chief of the *IEEE Network Magazine*. He has serves on the editorial boards of several international technical journals and the Founder and the Editor-in-Chief of *Wireless Communications and Mobile Computing Journal* (Wiley). He guest edited a number of special issues in the IEEE journals and magazines. He served as the IEEE Computer Society Distinguished Speaker, from 2003 to 2005.

SONIA KHAN received the bachelor's degree in computer science from the Department of Information Technology, The University of Haripur, in 2015. She is currently pursuing the M.Sc. degree in computer science with COMSATS University Islamabad, Abbottabad. Her current interests include fuzzy logic, the Internet of Things, mobile data offloading, and opportunistic networks with a particular emphasis on its delay tolerance.