IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON ARTIFICIAL INTELLIGENCE (AI)-EMPOWERED INTELLIGENT TRANSPORTATION SYSTEMS

Received November 25, 2019, accepted December 5, 2019, date of publication December 17, 2019,
date of current version December 27, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2960367

DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET

M. POONGODI[1], MOUNIR HAMDI[1], (Fellow, IEEE), ASHUTOSH SHARMA[2], MAODE MA[3], (Senior Member, IEEE), AND PRADEEP KUMAR SINGH[4]

[1]Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa Univeristy, Doha, Qatar
[2]School of Electronics and Electrical Engineering, Lovely Professional University, Phagwara 144411, India
[3]School of Electrical Electronic Engineering, Nanyang Technological University, Singapore 639798
[4]Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat 173234, India

Corresponding author: M. Poongodi (dr.m.poongodi@gmail.com)

This work was supported by the Qatar Foundation.

ABSTRACT It is essential for Vehicular Ad-hoc networks (VANETs) to have reliable vehicles for communication with vehicles. VANET is dynamical network where the vehicles frequently alter their place. Safe routing is of great essence at the time of routing process to fit in shared trust/belief involving these nodes. Occasionally, the malicious node transmits the counterfeit data amid other nodes. To find out trust/belief is deemed to be a difficult task when the malicious nodes try to distort the discovery of route or transmission of data within the network. Researchers have worked extensively to ensure a safe routing process with trust-oriented applications. We develop the framework based on trust with a fresh mechanism to determine DDoS attacks in VANET. The major trust elements in the evaluation of trust are frequency value statistics, trust hypothesis statistics, residual energy, trust policy, and data factor. Based on the trust elements, the generation of trust evaluation matrix takes place. We develop the suggested trust mechanism in an innovative manner to offer the security in a better manner by avoiding the trespassers in the network. The deterrence design by trust evaluation mechanism in combination with a clustering method is proficiently made use for the identification of the attacker and reduction of the price concerning detection method. The suggested system optimizes the utilization of a bandwidth without compromising the security of the nodes in the network.

INDEX TERMS DDoS, trust evaluation, secure routing, cluster, intrusion prevention.

I. INTRODUCTION

Vehicular ad-hoc network (VANET) [1] is a kind of infrastructure where the communication between the neighbouring vehicles takes place by Road Side Units (RSU) or Road Side Infrastructure using wireless network. Every vehicle in the network is equipped by two units which are Application Unit (AU) and On-Board Unit (OBU) considering vehicle as the network node. The nodes communicate among themselves with Vehicle to Vehicle communication (V2V) and also Vehicle to Infrastructure (V2I) communication can be attained through Road Side Unit (RSU) [2]–[4]. The primary focus is on to alleviate the Intelligent Transportation System (ITS) objective of this to provide the various applications such as infotainment, safety etc. The nodes in more number claim a variety of services over the network at the specified point of time in a range of applications. The service for the network can't be provided if a request exceeds the capability. The overwhelming of packets is not allowed. Since it provides only limited access of data at any point of time, the service request suffers from overload, if it receives the packet with higher payload which in turn it affects the network performance [5], [6]. The VANET infrastructure is depicted in Figure 1.

The road side units and vehicles communicate each other and acts as a transmitter and receiver. The communication between vehicles is highly dynamic and continuous in highways. The vehicles communication in the network establish for very short span of time. Thus, the vehicles are highly dynamic the network communication links rapidly connects and disconnects from the network [6]. VANET have high dynamic topology due to its network behavior. There is the highways and road which are predefined as it is already build makes the vehicle pattern predictable. And also the mobility pattern of vehicles also can be predicted with the layout and topology. There is high chance of uncertainty also in the

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

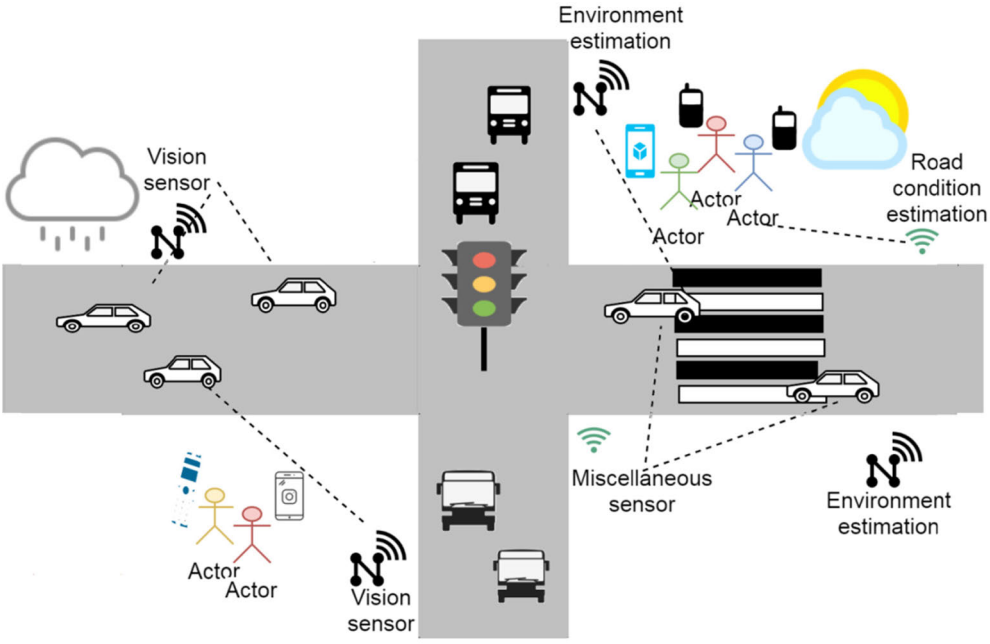

FIGURE 1. VANET infrastructure.

network due to lane structure, behavior of vehicle drivers, density of traffic and complete road layout. The nodes density also varies in different locations since it is varies in population and peak time, it can be more in highways than in remote areas. The peak time like office hours of that geographical location and office leaving time will be have more nodes density in the infrastructure. Hence, the design of protocol has been done considering this fact. The VANET node gets data from different RSUs and there is the chance of multiple hops to send the information between the nodes. Which in turn, it makes the network more vulnerable to various type of attacks especially Denial of Service (DoS) attack and Distribute Denial of Service (DDoS) attack.

In VANET, DoS attacks overwhelm the packets to a particular node or network, with the redundant information and messages, so that the services for the legitimate nodes get affected [6]. A DDoS attack can be made by zombies or automated attackers in large scale, so that legitimate users no longer can access the network. Owing to the characteristic of the VANET infrastructure like dynamic topology of network nodes and decentralization; recognizing the malicious attacks, unruly nodes and defective vehicles are challenging.

So as to overcome the above mentioned challenges, the trust oriented framework is developed with a new mechanism to identify DDoS attacks in VANET. The chief trust elements incorporated in the evaluation of trust are data factor, trust hypothesis statistics; frequency value statistics trust policy and residual energy. The evaluation matrix with reference to the trust components is generated as trust evaluation matrix. The proposed trust mechanism is designed in a novel way for providing the better security by preventing the intruders in the network. The deterrence design by trust evaluation mechanism in combination with clustering methodology is resourcefully utilized for the identification of the attacker and reduction of the expenditure concerning detection technique. The proposed system optimizes the utilization of bandwidth without compromising the security of the nodes in the network. To check the accomplishment of the suggested technique, a variety of network factors are taken into consideration namely as Average Latency (AL), Packet Delivery Ratio (PDR), Detection Rate (DR) and Energy Consumption (EC). In the recommended research study, the metric PDR is utilized to discern the number of data packets that are effectively sent at the destination. The mentioned factors are utilized to gauge how efficiently the data packets are sent from the resource to the end place.

The present study is divided into six segments: the Section II deals with the literature review. Section III explains Problem definition and provides the solution. Section 4 illustrates the suggested approach. While Section V reveals the results and analysis and the conclusion is presented in Section VI.

II. RELATED WORKS

VANET security cached up the attention of researchers in recent years to the greater extent [1], [7]. Despite, deep research studies being conducted with regard to security, there has been no reasonable research study to avert/alleviate the DoS and DDoS attacks in VANET setting. Consequently, we are more explicit and centered on this subject matter as given below.

In [8] this projected work, here the author has used the Dedicated Short Range Communication (DSRC) & revocation methods. The projected work here for detecting DDoS attack is on the basis of offender transfer that is target node receives messages and also obtained by a variety of locations with varied slot time for the transfer of the messages, in the meantime the offender endeavors to change the slot time and

converse with diverse vehicular nodes. The significant cause for this incidence is to create the network in lively and in reachable to the vehicular nodes or victims by bringing down the whole network down and demanding. DSRC consists of seven channels, and author has created the 4 classes and done precedence based sorting. Class 1 signifies the uppermost and class 4 symbolizes the least. However, few nodes in the infrastructure of VANET accept security messages at a specific timestamp, so it has been recognized that nodes are attacked, it can shield itself against DDoS and DoS attacks in the coming times.

The one more possible method to mitigate DDoS attack is the Traffic capacity and Bloom Filter [9]. This avoids spoofing of network addresses and protects against it. The measurement of traffic exposure is relied on the detection algorithm. The proposed detection algorithms are categorized into three phases. Phase 1 gather and segregates the data and given as the input for the phase 2. The phase 2 process the input from the phase1 and it checks for malicious node existence and stored in the database. Phase 3 entails the procedure of bloom filter by hash function, remarkably any malicious nodes was commenced by the phase 2 and it triggers an alarm, by which it transmits the information to the whole nodes in VANET.

The APDA (Attacked Packet Detection Algorithm) [9] and MVND (Malicious Node Detection Algorithm) [10] techniques are to alleviate the Denial and Distributed Denial of service attacks. The APDA methodology acquires aspects such as position, velocity, and time stamp to recognize malicious nodes. The system of identifying the dangerous nodes prior to the time of corroboration will minimize the stoppage of overhead which in turn enhances the security in VANET. Still, the MVND methodology is utilized to establish the malicious nodes prior to verification time by applying the hybrid network.

In this part, we are unfolding the current approaches which are presented on trust evaluations and establishment in VANETs. Trust evaluation model pursues a range of trust models and systems to set up trust among vehicles.

Hong *et al.* [11], elaborated on the establishment of trust management system in three facets, which affects the social media on network, policy control and proactive trust establishment. Characteristics of entry trust and data trust are utilized for Policy control. The past communication history of node vehicle is utilized for trust value alike traditional approach for Proactive trust. The third feature is Social trust which takes into account neighbor nearby vehicles evaluation and setting up trust amongst other vehicles.

Hortelano *et al.* [12], Trust management scheme has been established using the watchdog algorithm in this research work as a detection mechanism. The monitoring history is used primarily for detecting the malicious behavior of the nodes in this detection mechanism. The nearest neighbor nodes are sent with packets from the source vehicles has been monitored and trust values are measured accordingly. The system recommends communicating the packets through high trust nodes which has been stored in a trust table. If there is an issue with communication, the trust value of the node gets decreased and updated in the trust table. The disadvantage of the system is, it creates the collision in the network, and since monitoring history is high, the system is not considerably scalable to the big network.

Liao *et al.* [13], recommended measuring the trustworthiness of vehicles with incident reports in vehicle to vehicle communication and communicated to those vehicles. The trust worthiness of the system is evaluated with crowded sourcing capabilities. Individual vehicle broadcast of trust values done by the global view. The system can be enhanced in future with security and privacy can be done by including the unique ids and public key infrastructure.

Ding *et al.* [14], the co-operative method among the nodes used to initiate the trust tokens dynamically. The packet integrity is also achieved by using some cryptographic mechanism with symmetric and asymmetric approach. In sequence, the neighborhood watchdog algorithm is applied to check the packet validity by generating the tokens. The security of packets is increased and delay of communication is considerably decreased. Here, instant trust value has been measure at run time using the co-operative packet forwarding mechanism. The main disadvantage of this system is not considering the reward for the good nodes to enhance the performance in future.

III. PROBLEM DEFINITION

Flooding attack is a severe DDoS attack. The major objective of this attack is to formulate the destination node inaccessible or demote the correspondence all the way by the network affects the availability as shown in Figure 1.3.

Attacks of such kind characteristically directs to overloading of network. DDoS attacks are employed on idea of forcing the victim system to reset or supply reduction like as network bandwidth, computing power and operating system data structures such that couldn't offer its anticipated service to drivers or passengers. This is noteworthy problem; high probability of collapsed network is because of unreachable message to the drivers on road and as well it is very much significant to be taken into account, if there is any life critical information that requires to be corresponded to the vehicle driver. It also leads to major accidents if the communication between vehicles and infrastructure is unavailable [5].

DDoS attack is deemed to be vital means of threatening. In the current DDoS attacks, most complex methods are instigated by the intruders. To surmount this kind of multiple attack actions, integrative methods have to be deployed. DDoS attacks are complicated to be traced back effortlessly due to its nature of distribution. It is very much complex to trace and to notice the attacks. DDoS attack in VANET can be initiated in two varied state of affairs.

A. VEHICLE TO VEHICLE

Attackers from different location send the messages and flood the packets to the victim using different time slot. The

availability of the network is getting affected for genuine nodes due to the network suffers to reply for the flooding requests [6].

B. VEHICLE TO INFRASTRUCTURE

Another approach is that malicious nodes target the Road Side Unit. The malicious attackers overwhelm of flood the RSU, to make it unavailable for the communication for genuine nodes and it has been overloaded with the packets to be handled by attackers rather than legit nodes. Hence, the service gets disrupted [6].

The automated attack is at present rising and a lot more famous amidst the intruders to carry out the Denial attacks in the network devoid of every attempt. Owing to the availability of tools, any ordinary individual could attack in the network exclusive of any knowledge. The robust mechanism is necessary to surmount the DDoS attack to the larger amount. As VANET is very much active and decentralized network with responsive field of information and as well the purpose of VANET is extremely widespread in the sector of Intelligent Transportation system. It is significant to safeguard from the intrusion in the VANET infrastructure.

In maximum latest disbursed denial of service attacks, utmost sophisticated methods are implemented via the intruders. To overcome similar multiple attack events, collaborative approaches want to be carried out. DDoS attacks are hard to be traced lower back easily due to its allotted nature. This is even harder to find and to detect the assaults [11]. Hence, an modern detection mechanism is wanted to prevent the security failure of the network in VANET.

IV. PROPOSED TRUST BASED FRAMEWORK

The proposed trust based framework uses the evaluation mechanism to detect and isolate DDoS attack from VANET. Also, the clustering scheme is integrated in the structure for better intrusion prevention. It discovers the proper hierarchical structure considered as significant step for easy classification and prediction of attackers. The clustering of nodes by using trust scores obtained. The trust evaluation mechanism is known as the way of determining the trust score of each nodes based on the primitive trust parameters. In the proposed technique trust parameters defines trust policy in order to find the dominant cluster for secure communication.

The trust based framework identifies the highly secure dominant cluster to increase the PDR and EC by avoiding the re-sending of packets. Trust framework combines clustering and trust evaluation system. In this method, the dynamic clustering structure is maintained to provide a secure communication through the trusted nodes. In order to implement this idea, the trust algorithms are proposed. These algorithms are responsible for identifying the trusted path. These algorithms compute trust policy for secure communication.

In trust based framework, the incorporation of genetic algorithm is done for the deterrence of intrusion. It ascertains the appropriate hierarchical tree structure that develops vertically and horizontally. The vertical development at each phase includes two nodes to the leaf based on the heterogeneity when it is better than a threshold (TR) value acquired from the trust scores obtained. We predefine a threshold value from the trust value obtained to test the cluster separation initially. The horizontal development at every phase, the optimal number of sub clusters of the least level nodes is figured energetically. The continuation of the process takes place until the heterogeneity of all leaves is smaller than a threshold TR. The node's heterogeneity is computed from the deviation of score obtained from frequency and entropy.

The primitive trust components define trust policy in order to find the dominant cluster for secure communication. The trust evaluation module finds the highly secure dominant cluster to enhance the packet delivery ratio and decrease the energy consumption by avoiding the re-sending of packets.

In trust based framework, the trust worthiness of each node is evaluated by node behaviors. The trusted nodes in each hierarchical level are recognized as a dominant cluster and very much entitle them for the participation in routing. Scalability is achieved by clustering the nodes. Optimum number of clusters in a certain hierarchical structure is used to find the intruder efficiently.

The Trust based architecture for VANET is described in Figure 4.

In the Figure 2, trust based framework gives improved security by the safe correspondence by means of the trusted nodes henceforth making it difficult for the intruder to attack the network. The clustering stage is utilized here to find out the apt hierarchical tree structure by means of Dynamically Growing Self Organizing Tree (DGSOT). The DGSOT is planned to discover the hierarchical configuration of the nodes. Dynamic tree develops vertically as well as horizontally. When the heterogeneity is better than the threshold value, addition of two children is done to the leaf in the vertical growth. Proper number of sub clustered children is dynamically figured out in every horizontal growth through the trust values attained energetically. The process is sustains until the heterogeneity value is smaller than the threshold value.

A. TRUST EVALUATION MECHANISM

The trust aligned with reputation settles on the location of nodes in a hierarchical tree and distinguishes risks connected to the probability of recognizing and meeting the malicious activities. By and large, the idea of trust is being seen as a faith concerning the performance of nodes. Yet, the definition of an entity's trust is an indication of the degree to which a peer node would be truthful and trustworthy, safe, and figured out to be dependable in several interactions with the node. Thus, trust parameters are used to evaluate the other node's ability to fulfill an expected action, and a node can take benefit of this information to make decisions when it must decide a set of trustworthy nodes. A trust based framework is made as direct observations to evaluate the neighboring nodes. The views of intermediate nodes are utilized to ascertain the trust relations

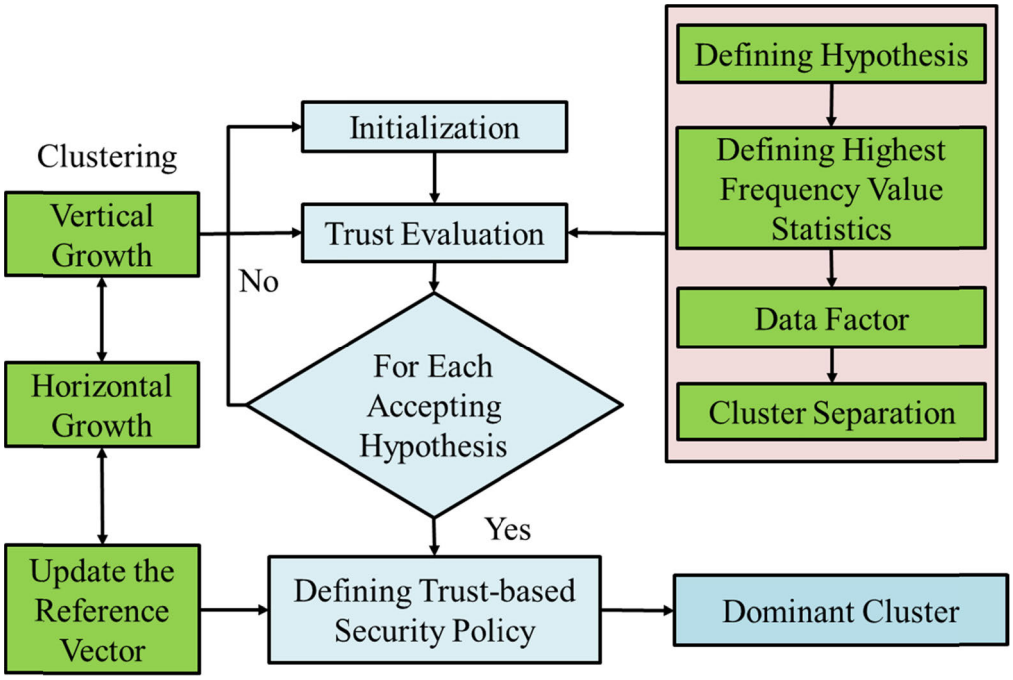

FIGURE 2. Trust based framework.

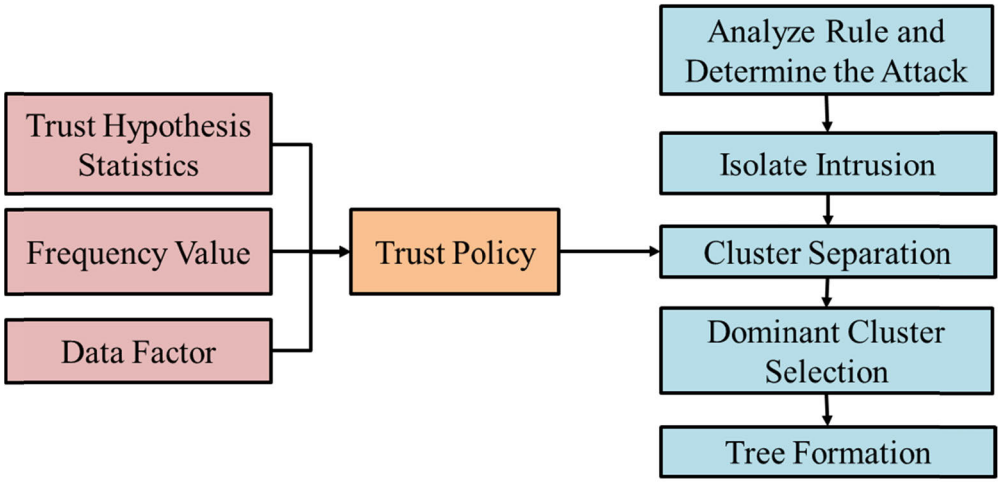

FIGURE 3. Trust evaluation mechanisms.

amid the two nodes which do not possess any former straight interactions.

The trustworthiness is self-assurance of one assessing a node with the other node in the network. Based on the viewpoint that the assessing node executes an action with regard to the distinct trust factors, regardless of the capability to manage or check other nodes present in the network. The trust evaluation factors are utilized to figure out the central clusters such as trust hypothesis statistics, frequency value statistics, data factor, derived trust policy and cluster separation as shown in Figure 5.

To provide efficient security solution on protection of data, secure routing and other network behavior. The trust computation and assessment are employed amongst the network nodes both computationally and logically. All of the node's examination of trust on other nodes is supposed to be on the basis of serious research and implication from straight observation of trust elements on other nodes, also node owner's inclination and strategy. So as to establish the appropriateness of the suggested method the trust oriented framework consists of the subsequent key mechanism namely trust hypothesis statistics, frequency value statistics, data factor and trust policy which are elaborated in the consequent subsections.

B. TRUST HYPOTHESIS STATISTICS

The statistic data denotes the past experience accumulated through the communications with other nodes. Each and every successful communication increases the trust index

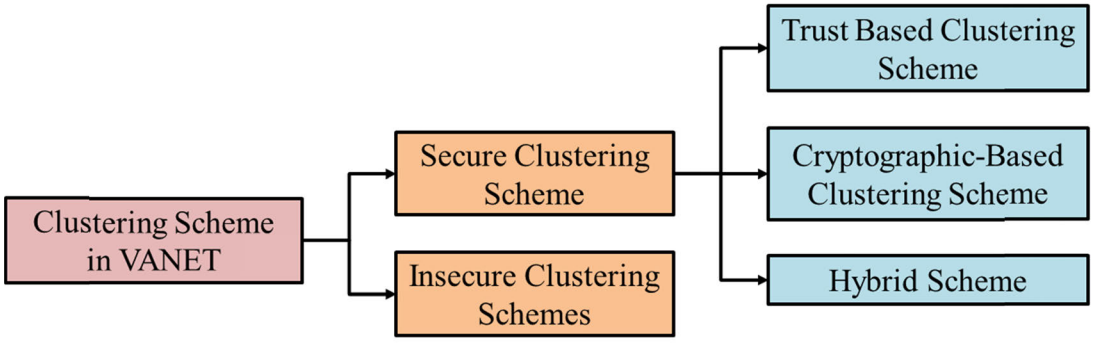

FIGURE 4. Various clustering schemes.

dynamically. The each communication failure all the way through the node in the network decreases the trust index attached to the node. The transmission trace algorithm is given as input to calculate the trust index dynamically. In a similar way human being's interactions, the amount of successful communication and the point of contentment are utilized to set up the trust level of an individual. The transmission trace algorithm given below is used to digitize the trust component values. The experience statistics value is digitized by using a Hypothesis Statistics algorithm.

Algorithm to obtain Transmission Trace

Input: Communication data

Output: Transmission of packet

Function Send_packets( )

Step 1: **Begin**

Step 2: Transmission_Packets ();

Step 3: **End.**

Algorithm for Hypothesis Statistics

Input: Transmission Trace

Output: Hypothesis Statistics

Function Hypothesis_Statistics ( )

Step 1: **Begin**

Step 2: **if** (packets are correctly transmitted between the pair of nodes i and j)
//Create Counter for Incrementing the Hypothesis value
Hypothesis values of the respective nodes will be incremented by one
Updated Hypothesis value = old value + 1

Step 3: **else** (number of dropped or delayed packets)
//Create a counter for decrementing the Hypothesis value
Updated Hypothesis value = old value −1
Digitized value of Hypothesis Statistics $HY_{(i,j)}$

$$HY_{(i,j)} = \frac{S_{(i,j)} - G_{(i,j)}}{S_{(i,j)}}$$

Where,
$S_{(i,j)}$ = Total number of communication count between nodes i and j.
$G_{(i,j)}$ = Communication failure count between nodes i and j.

Step 4: **End**

The above algorithm is responsible for determining the node's behavior on communication capacity of each pair of nodes to find the trust hypothesis statistics value to derive trust policy.

C. FREQUENCY VALUE STATISTICS

Frequency value statistics determines the successful transmission highest frequency of data at the specific instance of time. The trust evaluator nodes broadcast the high frequency of data in a unit of time holding the high frequency value statistics as mentioned in the below algorithm.

Algorithm for Frequency Value_Statistics

Input: Transmission Trace

Output: Frequency Value Statistics

Function FrequencyValue_Statistics ( )

Step 1: **Begin**

Step 2: **if** (packets are correctly transmitted between the pair of nodes i and j);
//Create Counter for Incrementing the frequency of packets($P_{(i,j)}$) at unit time T

Step 3: Initialize $t = 0, T$

Step 4: **if** ($T < t$)

Step 5: **if** (Successfully Transmitted packets)
$T = t + 1$
Updated frequency value = old value + 1

Step 6: **else** (number of dropped or delayed packets)
//Create a counter for decrementing the frequency Value
Updated Hypothesis value = old value − 1

Step 7: Digitized value of FrequencyValue_Statistics $FV_{(i,j)}$

$$FV_{(i,j)} = \frac{P_{(i,j)}}{T}$$

Where,
$P_{(i,j)}$ = Successful data transmission between nodes i and j.
T = time

Step 8: **End if**
Step 9: **End if**
Step 10: **End**

The above algorithm is responsible for the frequency of total successful communication on unit time, the Frequency statistics value is digitized by using an algorithm.

D. DATA FACTOR

Data Factor means that the likelihood of successful data packets being broadcasted, misplaced and obtained among the trust evaluator node i and j during communication.

Algorithm for Data Factor

Input: Transmission Trace

Output: Data Factor

Function **Data_factor ( )**
Step 1: **Begin**
Step 2: Transmission of packets ();
Step 3: Calculate Tot_{ps} = Total number of packet sent
Step 4: Intitalize a
Step 5: **if** (Successfully Transmitted packets)
Counter $a = a + 1$
Step 6: Packet lost rate computed
$Tot_{lst} = Tot_{ps} - a$
Step 7: Total number of dropped or delayed packets
// Decrementing data factor
Step 8: Transmitted packets = $Tot_{ps} - Tot_{lst}$
Step 9: Digitized value of Data Factor $DF_{(i,j)}$

$$DF(i,j) = \frac{Totps - Totlst}{Totps}$$

Where,
Tot_{lst} = Total Packet Loss.
Tot_{ps} = Total Packets Sent.

Step 10: **End**

The above algorithm is responsible for the data factor, the packet transmission between the nodes, the data factor value is digitized by using an algorithm.

Clustering: The various clustering schemes are mentioned in the Figure 6. The research work mainly focuses on trust based clustering network model.

E. CLUSTER SEPARATION

The projected network replica augments the network security by developing the examining authority of the concerned nodes. The monitoring is more efficient when nodes are clustered. The proper number of clusters in a hierarchical structure provides better security on analyzing the degree of potential attack. The high trusted node at each hierarchical level is identified as a dominant cluster for a secure way of communication in the network.

The flowchart illustrated in Figure 5 comprises of four stages. Initialization phase follow by Vertical growing phase, Horizontal growing phase, Winner and nearby reference vector updating phase. The process executed between the nodes of root and leaf is called as the learning process. The initial clustering performs the trust analysis and then refines the clusters. The reference vectors of every node are centroid of all data related with its leaf descendants. All nodes of hierarchical level form a Voronoi set (Kohonen 1998). The Cluster Separation (CS) at each hierarchical level is given as maximum value to the minimum value between two centroids. The optimal number of clusters in all hierarchical level is achieved by using the CS. The trust policy is defined based on the primitive trust parameters which are trust hypothesis statistics, frequency value statistics and data factor. The trust policy is used to conclude the dominant cluster dynamically at the each hierarchical stage of secure communication.

Algorithm – Clustering

Input: Trust Values

Output: Clustered tree

Function Clustering ( )
Step 1: **Begin**
Step 2: Initialization ();
Step 3: **if**(Horizontal Growing Flag (HGF) = true).
Step 4: Association of IP address with the System data
Step 5: **if** (Vertical Growing Flag (VGF) = True),
For heterogeneity > threshold T_R.
Set the HGF =value
Update the IP of neighborhood system
Step 6: **if** (Horizontal growing stop rule = unsatisfied)
HGF = true
Step 7: **else**(Set the HGF = false).
Update reference vectors of winner and its neighborhood
Step 8: The HGF of all lower levels < threshold T_R
Step 9: **End**

The clustered tree is formed from the trust values obtained by monitoring the behaviors of nodes and refining of clusters done periodically by the trust values obtained dynamically.

Algorithm – Cluster Initialization

Input: Trust values

Output: Initialization of Clustering of nodes

Function Initialization ( )
Step 1: **Begin**
Step 2: Create a tree has only one root node.
Step 3: Initialize the reference vector of the root node the centroid of the entire data
Step 4: Associate all data with the root

Step 5: Set the HGF = true
Step 6: **End.**

The modules of clustering algorithm is given in the above algorithms in which the cluster separation done dynamically based on the trust values and the dominant cluster is framed based on the trust policy.

Algorithm Vertical Growth

Input: Trust values

Output: Partial Clustered tree

Function Vertical_Growth ( )
Step 1: For (leaf heterogeneity > Threshold T_R)
Step 2: Change the leaf to a node
Step 3: Create two descendent leaves.
Step 4: Initialize the reference vector for the new leaves
Step 5: For (each New leaf)
Set the HGF = true /∗Learning∗/
Step 6: For (each input data)
Find winner
Step 7: Update reference vectors of neighborhood and its winner

Algorithm- Horizontal Growth

Input: Trust values

Output: Partial Clustered tree

Function Horizontal_Growth ( )
Step 1: **Begin**
Step 2: **For** (lowest level node)
Step 3: **If** (Horizontal growing stop rule = unsatisfied)
Step 4: HGF = true
Step 5: Add a child leaf to this node
Step 6: **else** (Delete a child leaf from this node)
Step 7: Set the HGF= false
/∗Learning∗/
Step 8: **For** (each input data)
Step 9: Find winner
Step 10: Update reference vectors of neighborhood and its winner
Step 11: While (HGF flag of all lower level nodes = false)
Step 12: While the heterogeneity of all leaf nodes is less than the threshold T_R
Step 13: **End**

Trust Policy: Dominant Clusters at all hierarchical level is recognized by the resultant trust policy energetically. The cluster consisting of maximum trust index is mentioned as the dominant cluster. The high trust node by using trust evaluation TE (i) on TE (j) is based on the security requirements viz. Hypothesis, routing message information from TE (j) and residual energy in TE (i) in the dw. The Network Security based on trust policy is defined in an algorithm given below:

The trust policy is measured through the trust components and dominant cluster is identified based on the trust policy as shown in algorithm.

Algorithm for Trust Policy

Input: Trust Parameters

Output: Trust Policy

Function Trust_policy ()
Step 1: **Begin**
Step 2: Compute Trust_policy
Step 3: Aggregate the Trust factors calculated
Step 4: Trust_policy $T_{(i,j)} = DF_{(i,j)} \times HY_{(i,j)} \times FV_{(i,j)}$
Where,
$DF_{(i,j)}$ = Data Factor
$HY_{(i,j)}$ = Hypothesis Statistics
$FV_{(i,j)}$ = Frequency Value Statistics
Step 7: **End**

Dominant Cluster: Dominant Cluster (DC) as shown in Figure 8 is with the maximum residual energy, trust hypothesis statistics, frequency value statistics and derived trust policy determined as given in Equation (1). The transmission of data by the dominant cluster will be more secure and highest data throughput.

$$DC_{(i,j)} = T_{(i,j)} \tag{1}$$

where, $DC_{(i,j)}$ and $T_{(i,j)}$ is Dominant Cluster and Trust Policy, respectively.

The cluster separation value is described as the max value to the min value between the two centroids and it is estimated as follows:

$$CS_{(i,j)} = \frac{E_{min}}{E_{max}} \tag{2}$$

where, E_{max} is maximum trust score, which represent maximum separation of centroids, E_{min} is minimum trust score, in which the centroids that are near to each other and CS is used to denote relative separation of the centroids.

Trust Evaluator Matrix: Trust matrix operates as a database and saves the knowledge utilized for the trust evaluation of nodes on the network. A matrix takes shape for storing the digitized values of trust elements analyzed for the cluster nodes from 1 to n groups as mentioned in the Equation (3).

$$TE = \begin{bmatrix} HY^1(i,j) & FV^1(i,j) & CS^1(i,j) & DC^1(i,j) & TE^1(i,j) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ HY^n(i,j) & FV^n(i,j) & CS^n(i,j) & DC^n(i,j) & TE^n(i,j) \end{bmatrix} \tag{3}$$

In trust based framework, the reliability of every node is assessed by node manners. The trusted nodes in every hierarchical level are recognized as a dominant cluster and

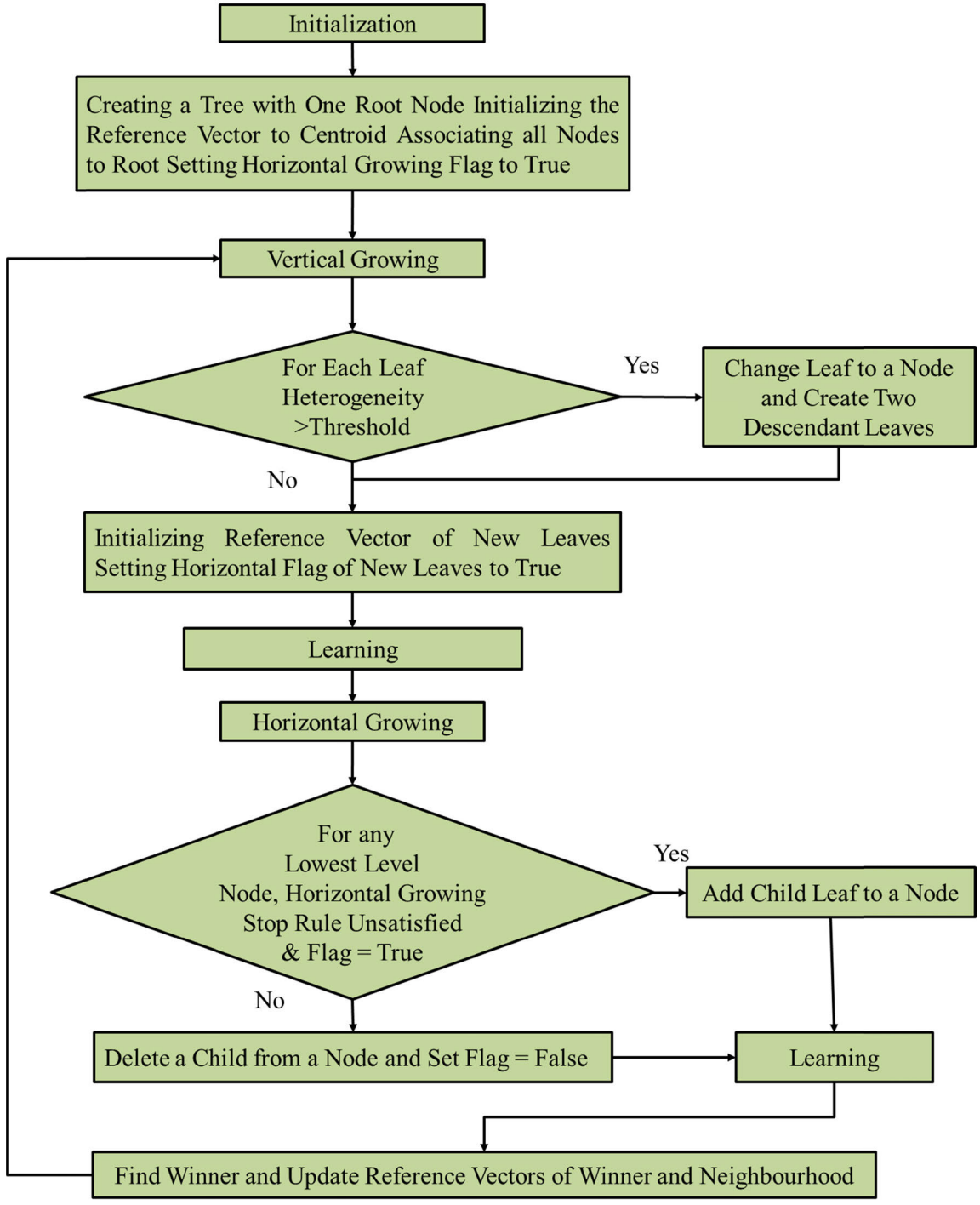

FIGURE 5. Flowchart of clustering algorithm.

extremely entitle them for the purpose of participating in routing. Scalability of the detection system is accomplished through the clustering of nodes. Suitable number of clusters at every hierarchical level is utilized to figure out the intruder proficiently.

V. IMPLEMENTATION AND RESULTS

A detailed simulation model based on NS-2.28 under Ubuntu environment is represented in the section V. A comparison between the suggested Trust based Framework and the prevailing systems is made in various network set-up. The experimentation is carried out to exhibit the competence of the proposed trust based framework.

A. COMPARISON OF PROPOSED WORK WITH THE EXISTING TECHNIQUE

In this work, the analysis, and implementation of DDoS are carried out. In order to evidently analyze the performance of

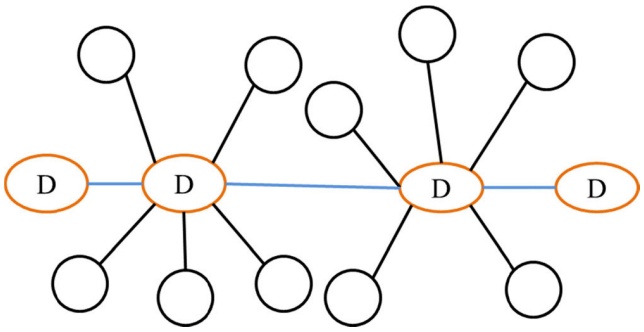

FIGURE 6. Dominant cluster selections.

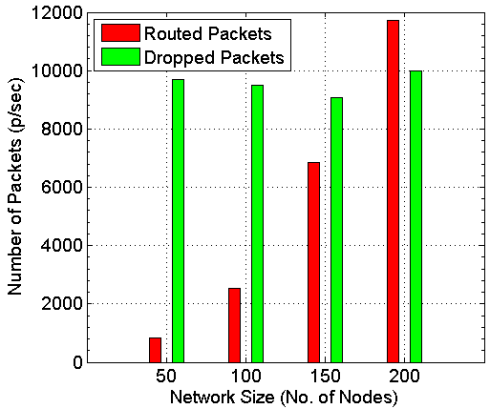

FIGURE 7. Routed vs. dropped packets in AODV.

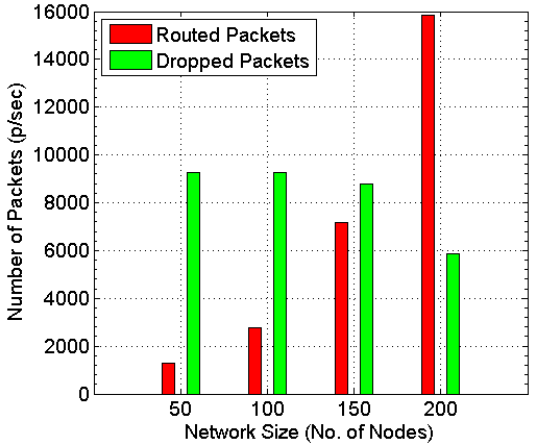

FIGURE 8. Routed vs. dropped packets in firecol.

the proposed work the following comparison techniques are implemented:

1) T1-ANALYSING DDOS AODV
2) T2-ANALYZING FIRECOL TECHNIQUE
3) T3-ANALYZING TRUST BASED FRAMEWORK

For all the above mentioned techniques, a variety of types of network size are utilized in order to know the activities and effect of DDoS attacks on the network size. Table 1 displays the performance of the AODV DDoS. In technique T1, the experiments have been executed with malicious nodes in AODV, with changeable network sizes.

1) T1-ANALYSING NORMAL AODV UNDER DDoS ATTACK

In Table 1, the calculated values are tabularized in the case of the DDoS attack on AODV protocol. All of the simulations are run three times, and the average values are tabularized.

TABLE 1. DDoS attack analysis on AODV.

Protocol	Nodes	Routed Packets	Dropped Packets
AODV	50	843	9700
	100	2527	9509
	150	6851	9083
	200	11734	9997

From the Table 1 mentioned above, the subsequent interpretations are done: Various network sizes are regarded as 50,100,150 and 200. The Figure 5.6 shows the performance of the DDoS attack for the AODV under different network sizes. The dropped packets are augmented from 9,700 p/sec to 9,997 p/sec when the network comprises of malicious nodes in the network.

2) T2-FIRECOL TECHNIQUE UNDER DDoS

In Table 2, all the calculated values in the case of the Firecol detection system under the DDoS attack are tabularized. All the simulations were run three times and the average values are tabulated.

TABLE 2. DDoS attack analysis on AODV.

Protocol	Nodes	Routed Packets	Dropped Packets
Firecol Technique	50	1265	9278
	100	2768	9268
	150	7170	8764
	200	15863	5868

The routed packets increases from 1265 p/sec to 15863 p/sec when the application of Firecol detection technique is carried out under DDoS attack. The Figure 8 showcases the performance of the Firecol detection technique under diverse network sizes.

3) T3-ANALYZING TRUST BASED FRAMEWORK

Table 3 shows the tabulated values that have been measured in the case of the trust based framework under the DDoS attack. Every the simulations were run three times and the average values are tabularized.

TABLE 3. Analysis of the trust based framework.

Protocol	Nodes	Routed Packets	Dropped Packets
Trust Based Framework	50	1792	8751
	100	4332	7704
	150	9082	6882
	200	18688	3043

The routed packets increased from 1792 p/sec to 18688 p/sec when the proposed Trust based Framework is implemented under DDoS attack.

The Figure 9 exhibits the performance of the projected trust based framework under a variety of network sizes. A comparison is made between the suggested trust based

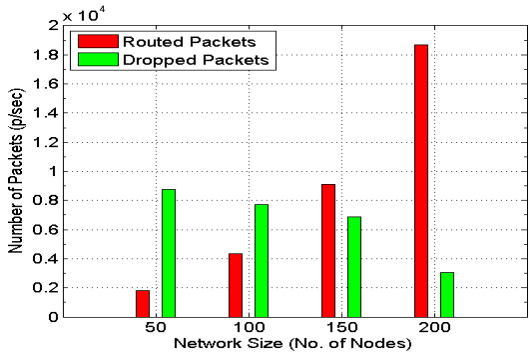

FIGURE 9. Routed vs. dropped packets in trust based framework.

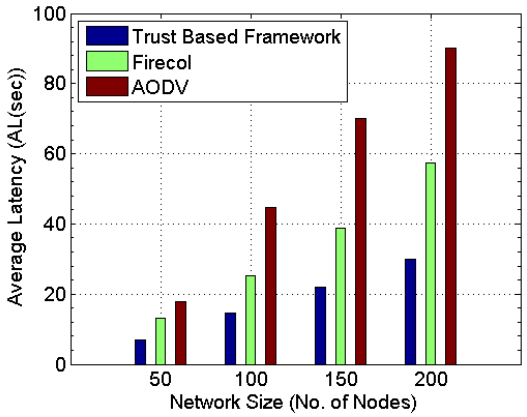

FIGURE 10. Comparison of the average latency.

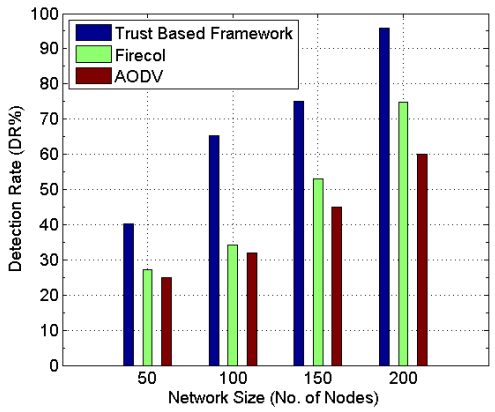

FIGURE 11. Comparison of the detection rate.

framework and the prevailing methodologies Firecol and AODV. The suggested technique enhances the PDR in comparison with the other prevailing techniques, as mentioned in Figure 9. From the Figure 11, it is very clear that the suggested method considerably enhances the performance of the PDR while comparing it with other techniques prevailing as given in Figures 7 and 8.

Figure 10 gives a comparative picture of the AL. After detecting the malicious nodes, the suggested technique shuns routing by means of the malicious node, and the AL is decreased in the suggested technique.

Figure 11 estimates the DR. The capability to detect the intrusion in the network through the proposed technique is

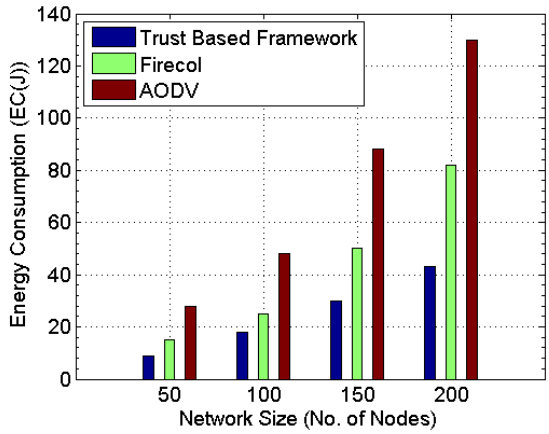

FIGURE 12. Comparison of the energy consumption.

augmented. The detection rate is elevated in comparison with the prevailing methodologies.

Lastly, the Figure 12 exemplifies that the energy consumption for data transmission process is condensed in the network where the projected technique has better lifetime in comparison with the other existing techniques.

From these results, it is evident that the proposed trust evaluation technique performs considerably better than the existing techniques.

VI. CONCLUSION

In this research work, a new methodology projected using the trust mechanism in combination with cluster mechanism to capably categorize the attackers to segregate the DDoS attacks in VANETs. Initially, the density based attack analyzer is used to analyze the network performance, when the attacks occur. It is revealed that the suggested technique develops the PDR in contrast to the prevailing techniques. Furthermore, that the projected technique decreases the AL and EC. The trust based framework is suggested and contrasted with prevailing techniques. The DR for the suggested trust evaluation technique is 95.8%. The DR for prevailing technique Firecol is 74.9% and AODV is 60%. From this it is noticed that the suggested trust evaluation technique enhances the recognition rate appreciably. When the network consists of malicious nodes, the PDR for the suggested trust evaluation technique is 86%. The PDR for prevailing Firecol is 73% and AODV is 54%. From this it is noticed that the suggested technique enhances the PDR extensively. When the network comprises of malicious nodes, the AL for AODV is 90 s, for Firecol technique is 36.1 s and for suggested trust framework AL is 30 s. When the network comprises of malicious nodes, the EC for AODV is 130 J, Firecol Technique is 82 J and for suggested trust evaluation technique EC is 43 J. From this it is clear that the suggested trust evaluation technique has very low EC. Therefore the suggested technique segregates malicious nodes and moves via normal nodes. The simulation results based on the experiments exemplify the originality and the efficiency of the suggested technique.

ACKNOWLEDGMENT

This work was supported by the Qatar Foundation.

REFERENCES

[1] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.
[2] I. Yaqoob, I. Ahmad, E. Ahmed, A. Gani, M. Imran, and N. Guizani, "Overcoming the key challenges to establishing vehicular communication: Is SDN the answer," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 128–134, Jul. 2017.
[3] I. Ahmad, R. M. Noor, I. Ali, M. Imran, and A. Vasilakos, "Characterizing the role of vehicular cloud computing in road traffic management," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 5, 2017, Art. no. 1550147717708728.
[4] I. Ahmad, U. Ashraf, and A. Ghafoor, "A comparative QoS survey of mobile ad hoc network routing protocols," *J. Chin. Inst. Eng.*, vol. 39, no. 5, pp. 585–592, 2016.
[5] L. Li and G. Lee, "DDoS attack detection and wavelets," *Telecommun. Syst.*, vol. 28, nos. 3–4, pp. 435–451, 2005.
[6] C. Buragohain, M. J. Kalita, S. Singh, and D. K. Bhattacharyya, "Anomaly based DDoS attack detection," *Int. J. Comput. Appl.*, vol. 123, no. 17, 2015.
[7] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017.
[8] A. Sinha and S. K. Mishra, "Preventing VANET from DOS & DDOS attack," *Int. J. Eng. Trends Technol.*, vol. 4, no. 10, pp. 4373–4376, 2013.
[9] K. Verma and H. Hasbullah, "Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in VANET," *Secur. Commun. Netw.*, vol. 8, pp. 864–878, Mar. 2015.
[10] S. A. Ghorsad, P. P. Karde, V. M. Thakare, and R. V. Dharaskar, "DoS attack detection in vehicular ad-hoc network using malicious node detection algorithm," *Int. J. Electron., Commun. Soft Comput. Sci. Eng.*, vol. 3, p. 36, 2014.
[11] X. Hong, D. Huang, M. Gerla, and Z. Cao, "SAT: Situation-aware trust architecture for vehicular networks," in *Proc. 3rd Int. Workshop Mobility Evolving Internet Archit.*, Aug. 2008, pp. 31–36.
[12] J. Hortelano, J. C. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs," in *Proc. IEEE Int. Conf. Commun. Workshops*, May 2010, pp. 1–5.
[13] C. Liao, J. Chang, I. Lee, and K. K. Venkatasubramanian, "A trust model for vehicular network-based incident reports," in *Proc. IEEE 5th Int. Symp. Wireless Veh. Commun. (WiVeC)*, Jun. 2013, pp. 1–5.
[14] Q. Ding, X. Li, M. Jiang, and X. Zhou, "Reputation-based trust model in vehicular Ad Hoc networks," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2010, pp. 1–6.
[15] H. Hartenstein and L. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 6, pp. 164–171, Jun. 2008.
[16] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "Secure and efficient trust opinion aggregation for vehicular ad-hoc networks," in *Proc. IEEE 72nd Veh. Technol. Conf.—Fall*, Sep. 2010, pp. 1–5.
[17] Y.-C. Wei and Y.-M. Chen, "An efficient trust management system for balancing the safety and location privacy in VANETs," in *Proc. IEEE 11th Int. Conf. Trust Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 393–400.
[18] T. Gazdar, A. Rachedi, A. Benslimane, and A. Belghith, "A distributed advanced analytical trust model for VANETs," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 201–206.
[19] R. R. Sahoo, R. Panda, D. K. Behera, and M. K. Naskar, "A trust based clustering with ant colony routing in VANET," in *Proc. 3rd Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Jul. 2012, pp. 1–8.
[20] Y. Chen and Y. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," *J. Commun. Netw.*, vol. 15, no. 2, pp. 153–163, Apr. 2013.
[21] B. Pooja, M. M. Pai, R. M. Pai, N. Ajam, and J. Mouzna, "Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," in *Proc. Asia–Pacific Conf. Comput. Aided Syst. Eng. (APCASE)*, 2014, pp. 152–157.
[22] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for VANET," *Int. J. Netw. Secur. Appl.*, vol. 5, no. 5, pp. 95–102, 2013.
[23] S. U. Rehman, M. A. Khan, T. A. Zia, and L. Zheng, "Vehicular ad-hoc networks (VANETs)-an overview and challenges," *J. Wireless Netw. Commun.*, vol. 3, no. 3, pp. 29–38, 2013.
[24] H. V. La and A. Cavalli, "Security attacks and solutions in vehicular ad Hoc Net-works: A survey," *Int. J. Netw. Syst*, vol. 4, no. 2, pp. 1–20, 2014.
[25] A. Quyoom, R. Ali, D. N. Gouttam, and H. Sharma, "A novel mechanism of detection of denial of service attack (DoS) in VANET using malicious and irrelevant packet detection algorithm (MIPDA)," in *Proc. Int. Conf. Comput., Commun. Autom.*, May 2015, pp. 414–419.

M. POONGODI received the B.Tech. (I.T) degree from Anna University, Chennai, the M.E. (CSE) degree from St. Peter's University, and the Ph.D. degree in information security from Anna University. She is currently pursuing Postdoc with Hamad Bin khalifa University, having expertise in many research areas. She has teaching experience of more than five years. Her many cited publications in highly indexed journals talks about her vast knowledge and skill set in the blended areas, such as network security, the IoT, machine learning, and deep learning. Her research interest is also extended in the areas of network analysis using social networking, mobile computing, Web services, 4G communication, cloud computing, and information security through anomaly detection. She is a renowned expert in networks field and a mass stunning speaker who has inspired a lot of students on network simulation through her hands on experience sessions. Many students have been done their B.E., M.E., M.Tech. and M.C.A. projects. She from Hamad Bin Khalifa University having expertise in many research areas.

MOUNIR HAMDI received the B.S. degree (Hons.) in electrical engineering (computer engineering) from the University of Louisiana, in 1985, and the M.S. and Ph.D. degrees in electrical engineering from the University of Pittsburgh, in 1987 and 1991, respectively. He was a Chair Professor and a Founding Member of The Hong Kong University of Science and Technology (HKUST), where he was the Head of the Department of Computer Science and Engineering. From 1999 to 2000, he held visiting professor positions at Stanford University and the Swiss Federal Institute of Technology. He is currently the Founding Dean of the College of Science and Engineering, Hamad Bin Khalifa University (HBKU). His area of research is in high-speed wired/wireless networking, in which he has published more than 360 publications, graduated more 50 M.S./Ph.D. students, and awarded numerous research grants. In addition, he has frequently consulted for companies and governmental organizations in the USA, Europe, and Asia. He is a Fellow of the IEEE for his contributions to design and analysis of high-speed packet switching, which is the highest research distinction bestowed by IEEE. He is also a frequent keynote speaker in international conferences and forums. He is/was on the editorial board of more than ten prestigious journals and magazines. He has chaired more than 20 international conferences and workshops. In addition to his commitment to research and academic/professional service, he is also a dedicated teacher and a quality assurance educator. He received the Best 10 Lecturer Award and the Distinguished Engineering Teaching Appreciation Award from HKUST. He is frequently involved in higher education quality assurance activities as well as engineering programs accreditation all over the world.

ASHUTOSH SHARMA received the M.Tech. and Ph.D. degrees in electronics and communication engineering from the Jaypee University of Information Technology, Waknaghat, India, in 2019 and 2016, respectively. He is currently working as an Assistant Professor with the School of Electronics and Electrical Engineering, Lovely Professional University, India. He has published more than 30 research articles in reputed SCI/SCOPUS journals and conferences. His topics of interest in research are SLA and QoS in communication, risk and performance modeling of the network, vehicular ad hoc networks (VANETs), UAV, cloud computing, machine learning, and security in smart cities. He has served as a Reviewer and Editor for several journals, such as the IEEE Communication Letters, the *Journal of Supercomputing*, IEEE Access, Elsevier, FGCS, Suscom, CEE, and COMCOM.

MAODE MA received the B.E. degree in computer engineering from Tsinghua University, in 1982, the M.E. degree in computer engineering from Tianjin University, in 1991, and the Ph.D. degree in computer science from The Hong Kong University of Science and Technology, in 1999. He is currently a tenured Associate Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. He has extensive research interests, including wireless networking, wireless network security, and optical networking. He has published more than 130 international academic research articles on wireless networks and optical networks. He has been a member of the technical program committee for more than 110 international conferences. He has been the technical track chair, the tutorial chair, the publication chair, and the session chair for more than 50 international conferences. He serves as an Associate Editor for the IEEE COMMUNICATIONS LETTERS, an Editor for the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, and an Associate Editor for the *International Journal of Wireless Communications and Mobile Computing*, the *Journal of Network and Computer Applications*, *Security and Communication Networks*, the *International Journal of Vehicular Technology*, the *Journal of Computer Systems, Networks, and Communications*, and the *International Journal of Computer and Information Technology*.

PRADEEP KUMAR SINGH received the M.Tech. (CSE) degree (Hons.) from GGSIPU, New Delhi, India, and the Ph.D. degree in computer science and engineering from Gautam Buddha University (State Government University), Greater Noida, India. He is currently an Assistant Professor (Senior Grade) with the Department of Computer Science and Engineering, Jaypee University of Information Technology (JUIT), Waknaghat. He has published nearly 85 research articles in various international journals and conferences of repute. He has received three sponsored research projects grant from the Government of India and the Government of Himachal Pradesh worth rupees 25 Lakhs. He has edited eight books from Springer and Elsevier and also edited several special issues for SCI and SCIE journals from Elsevier and IGI Global. He has Google scholar citations of 411, H-index of 12, and i-10 Index of 15 in his account. He is a Life Members of the Computer Society of India (CSI) and IEI and promoted to the Senior Member Grade from CSI and ACM. He is an Associate Editor of the *International Journal of Information Security and Cybercrime* (IJISC), a scientific peer-reviewed journal from Romania.