A hybrid node-to-node trust probability based clustering framework for VANETs

NagaRaju M, Research Scholar, Dept of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India.
Dr Amarendra K, Professor, Dept of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India.

Article History: Received: 03.04.2023 Revised: 11.05.2023 Accepted: 19.06.2023

Abstract

Vehicular Adhoc Networks(VANETs) plays a vital role in many real-time applications due to its topology structure, network size and communication. Node clustering , node inter clustering and intra clustering and node trustiness are the key parameters to improve the overall VANET efficiency. Conventional VANET clustering models are difficult to find and create the clusters based on dynamically changing locations and velocities. Also, in the intra clustering variation, as the number of cluster members are increasing in size, it is difficult create dynamic clusters based on the network topology. In order to overcome these issues, a hybrid VANET clustering framework is implemented based on node properties and trust values. Experimental results show that the present model has better efficiency than the traditional models.

Keywords: dynamic vehicle initialization, trust probability , Node trustiness, path planning.

1. Introduction

Vehicular Adhoc Networks (VANETs) are an application for Mobile Adhoc Networks (MANETs) that can make roads safer and make people more comfortable. Recently, researchers in wireless networks and mobile communications became interested in VANETs because they are different from MANETs in terms of their characteristics, challenges, applications, and architecture [1]. Vehicular network, also called VANET or vehicular ad hoc network, is an emerging wireless ad hoc technology that can be used for security, speed, and fun. Researchers are drawn to it because of this. But VANET shows that the irregular connectivity is due to the many changes in the topology of vehicular networks and the mobility of networks. In VANET, it's not easy to find a link between peers. This unique thing about VANET poses a hard question to the routing method: how to find the routes even though the connections aren't always the same. There have only been a few studies that answer the question above. One way to solve the problem is to keep and move the data until it gets to the right receiver. This method is sometimes called "carry and forward." When it gets to its destination, the data is given to it. The speed of the message may be the same as the speed of the vehicle, which is slower than the speed of wireless communication. Since the packet doesn't last very long, there is less chance that it will get to its destination. We've also seen that if a junction node has a chance to fix up a chosen path, it's more likely to send a signal through a wireless medium. Also, the incoherent node is less likely to meet a mobile node that is linked to it within the limited life time data. This is why the carryforward scheme is so bad, both in terms of how well it works and how long it takes from beginning to end. VANETs are used in situations that are different from the norm. As the nodes move around more, the time it takes to send a message is cut down. Vehicles moving in the same direction and at about the same speed can stay connected for longer periods of time. The network works well both in urban settings and on highways [2]. Buildings in the middle of city streets often get in the way of radio signals, which makes city roads a unique kind of geographical restriction. Traffic in cities is also affected by the way streets are named and by traffic and other signals. Due to how fast vehicles can move, there aren't many of them on highways. The "number of vehicles per unit distance" is used to figure out how much traffic there is. The density has a big effect on how well the road works and how fast the vehicle node moves. When density is low, vehicles should move faster, and when density is high, they should move more slowly. In the case of a roadblock, both the number of cars and their speed are almost steady. Clustering is the same as the problem of putting together a Minimum Dominating Set (MDS). A node in an MDS can be part of either a Dominating Set (DS) or an Ordinary Set (OS). The nodes in DS are called Child Nodes (CHs), and the nodes in OS are called Member Nodes (MNs). Every node in the OS is always linked to a node in the data store (DS). This is called "Topology Control and Management," and it gets rid of redundant topology information by creating node hierarchies. This helps and simplifies the next steps in networking [3]. A Connected Dominating Set (CDS) is a DS where the subgraph made up of only the nodes in the DS (and the edges between them) is connected either directly or through gateway nodes. [4] say that clustering is an NP-hard problem, even if you know everything there is to know about topology. Because of this, a lot of research goes into making efficient approximation clustering algorithms and distributed heuristics to cut down on flooding and broadcasting and, in turn, make the routing protocol itself easier to compute. [5] all predicted that the number of outcomes would go up in the case of different types of routing. VANETs are very different from MANETs in many ways, such as the way they are designed for mobility and how quickly their topology can change. Because of this main difference, the way routing works in MANETs now can't be directly linked to VANETs. In the first part of this look, the projections for the VANET routing mechanism are looked at. [6] also describe broadcast approaches (2010). In general, there are three things that need to be taken into account when a node is mobile: its position, the direction it is moving in, and its speed. Among these, direction has been found to be an important factor in choosing the next hop during the route-finding phase. In this model, the proposed solution is to choose the next-hop option from the nodes that are in the same direction as either the source or the destination. The parameter of position was also taken into account when choosing the next hop. People have pushed for the DAODV protocol to fix the problems with the standard AODV protocols. The main goal of the DAODV protocol is to make routes that are more stable, especially in applications like VANETs that require a high rate of mobility of the nodes. In the proposed method, the next hop is chosen based on direction and location, which are two important metrics. This is done during the route discovery phase[7][8].

2. Related Works

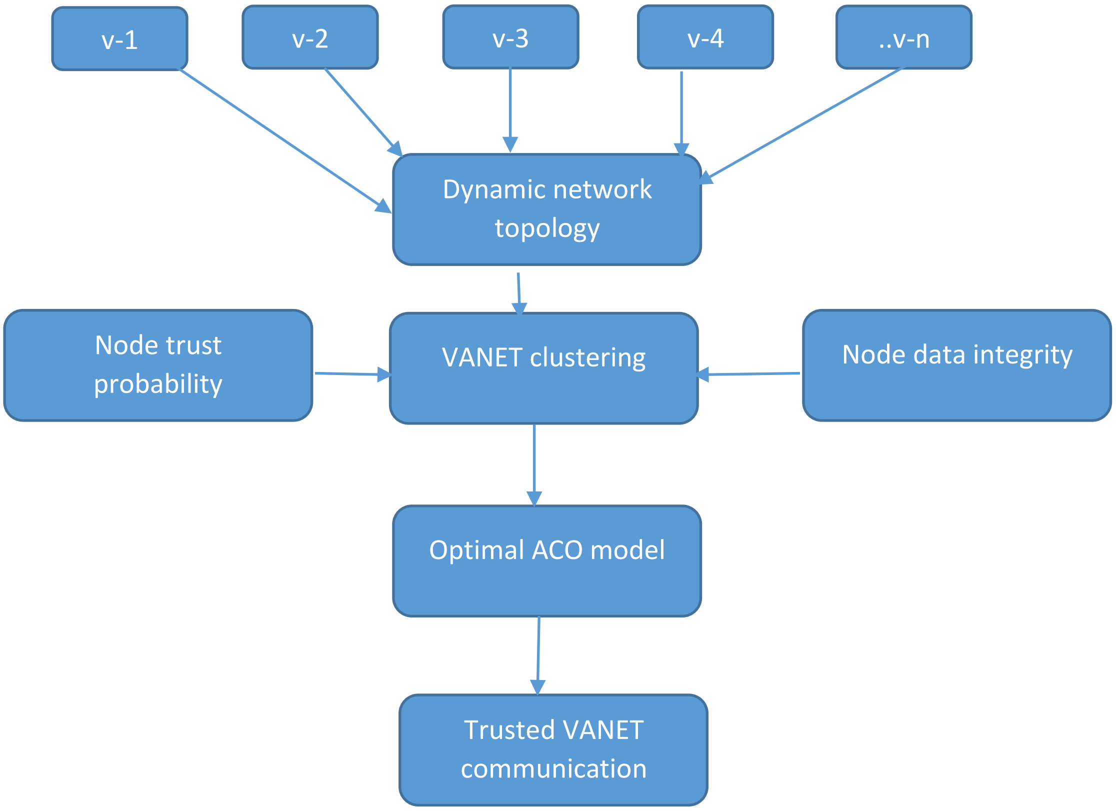
[9] came up with a method called Temporary Parallel Route Recovery, which can make a temporary parallel route between the participating nodes, especially when links fail. The

proposed mechanism uses a unique method of propagation that creates a special way to find parallel routes that can be used in real-time applications to send out data that needs to be sent quickly. Here, a buffer is given to all the source-to-destination nodes so that the data being sent won't be lost completely if the link fails. The buffer in the nodes saves the data packets, which the nodes then send on demand without losing any information, depending on the type of information being sent. [10] tried to solve one of the most difficult problems in research: how to make routing algorithms that can be scaled up and are reliable enough to deal with the fact that vehicles move around a lot and often break their paths. Fast Restoration On-demand Multi-path Routing (FROMR), a multi-path routing protocol, is recommended for use in VANETs. FROMR is different from the other research methods that focused on the disjointness. Instead, it focuses on building an alternative route right away if the original path breaks because a link fails or for some other reason. FROMR further divides the world into square grids of the same size, so that the number of control messages can be cut down and the path can be made stronger. A grid leader is chosen for each grid. The leader of the grid is the car that is most likely to stay in place for the longest amount of time. Because of these chosen leaders of grid, the route was found, kept up, and put back together. The results of the experiments and simulations show that the proposed FROMR protocols perform much better than the standard AODV protocols in terms of the ratio of packet delivery, throughput, route lifetime, and control overhead. [11] are aware of how mobile VANETs are and how often communication breaks down as a result. So that this problem can be solved, a hybrid protocol has been made that uses the best parts of both the reactive protocol and the geographic routing based on location. With this method, broken connections between the Road Side Unit (RSU) and each vehicle will be fixed. As part of the ADO approach, the source is usually told when a link breaks. But this paper describes a method called the Hybrid Location-Based Routing protocol that lets the nodes in the middle fix the broken link locally. When a new route from source to destination is set up, a lot more power is used. This is not the case here. The mobile node sends out the beacons periodically. The beacons have the IDs and current locations of the vehicles. These beacons help create neighbours and then update the neighbor-table, which has the vehicles' IDs and where they are located. [12] know that VANETs have to deal with a number of problems, such as choosing the best route, making sure alert messages are sent securely, and dealing with traffic jams. So, a solution has been put forward to deal with the serious problems, such as secure data transmission using Pretty Good Privacy (PGP), which ignores the extra load and solves the problem of traffic congestion on the network. To choose a dynamic route in the VANET, a hybrid protocol is used. This protocol combines the routing protocols of AODV and AOMDV. The required certificates are given to each node by a centralised authority, which also checks the node's certification. Wireless communication technologies have been used in VANETs to let vehicles talk to each other and to connect vehicles to infrastructure. In this paper, some protocols for wireless access in vehicles, such as standard 802.11p, P1809, CALM, MBWA, Cellular System, Bluetooth, Microwave, WiMAX, and ZigBee, are looked at in a broad sense. It also compares and analyses different wireless standards. This system makes it possible for potential forwarders to resend a message they have already received after a certain amount of time has passed, which depends on how far away they are from the previous forwarder. So, messages should be sent first to the nodes that are farther away. Also, a scheme for intelligent flooding based on a timer for VANETs, called a suppression mechanism, stops a competing node from sending the same message again if it hears a copy of it. This timer-based mechanism seems like it would work well in the highly changing world of vehicles in VANETs, where each node only needs to know its own position. But most of these methods don't completely stop the transmission of these duplicated messages because the suppression method itself has problems that can't be fixed. Also, any attempt to process the message before it is rebroadcast, such as updating the content of the message, could cause more problems because the time expiration set by the content mechanism determines when the message should be forwarded. [13-15] explain that the main goal of traditional routing protocols in VANETs is to find the path from the source node to the destination. The proposed method used the single path to find the route, and it doesn't take into account the process of finding the route. This kind of behaviour causes links to break and adds to the network's workload by making the network's overhead and delay longer. [16] came up with the idea of multipath routing to find different ways to get from the source to the destination. The nodes in this network have information about all the paths. This helps the network be used more efficiently and makes it easier for the routing system to adapt to different situations. Based on the properties of the nodes, multipath routing can be divided into three types: Node disjoint multipath routing, Link disjoint multipath routing, and Non disjoint multipath routing. In node disjoint multipath routing, neither the nodes nor the links share information about the path. In Link disjoint multipath routing, the links don't share the path information. In Non-disjoint multipath routing, all of the nodes and links in the network share information about the path. The non-disjoint multipath routing uses fewer resources than the disjoint multipath routing. The time it takes to find a route in non-disjoint multipath routing is less than in disjoint multipath routing. Due to the shared links and nodes, non-disjoint multipath performs worse in terms of fault tolerance. Here are three types of multipath routing and how well they handle problems: Link and Non-disjoint multipath routing have the worst fault tolerance, while Node-disjoint multipath routing has good fault tolerance. Link and Non-disjoint multipath routing involve the nodes in finding the best route. If something goes wrong with an intermediate node, the whole network will fail. Multiple description coding schemes are the name for the ways of coding. They came up with the idea of using disjoint and braided multipath routing to make the routing process better in multipath routing. In many multipath routing protocols, only the network layer is used to evaluate how well the routing works. Multipath routing protocol performance can also be judged by how well the MAC layer and paths work together. In VANETs, multipath routing is always a good idea. If someone says "no," the downsides need to be thought about. Also, the cost of multipath routing and the performance metrics that can be used to improve the performance of multipath routing need to be looked into. Many researchers have tried to solve these problems by focusing on this area, but their research is based on assumptions that don't give exact results and can only be used to explain the theory. So, the questions about how to choose the best path in multipath routing remain the same. In VANETs, if a link fails, a different path is chosen to avoid the problem, and the Quality of Service is improved with a route-assisted mechanism. The number of failed links will go down because of this route-assisted mechanism. In Wimax-based VANETS, the handover latency is kept to a minimum by using cross-layer design, and the handover latency is also reduced by the scanning latency. Adaptive Channel Scanning is all about choosing the least amount of time to scan for a mobile subscriber. Through the serving base station, the mobile subscriber will get information about how long each base station is expected to take to scan. The mobile subscriber chooses as its target base station the base station that takes the least time to scan. The cell ID-based handover method is used in multi-hop relay networks to cut down on the time it takes to switch from one cell to another. Ant colony optimization (ACO) is one of the best algorithms in the field of systems that are based on natural processes. ACO is used to solve problems like sequential ordering, the travelling salesman problem, and the open shop problem. ACO algorithms are used to solve problems with selecting features in a good way. With the help of ants, the ACO algorithm is used in VANETs. Packets stand for the ants, and some rules are written on the packets. These packets are sent through the IP-based network that Dong et al. talk about (2014). The most important thing to think about in the PSO is how people interact with each other and how smart they are. Here, the birds that learned from their own experience are said to have done "local search," while the birds that learned from what other people had done are said to have done "global search." [17] wrote about the benefits of PSO, which include being good at global search, easy to use, and having a small number of parameters to change. The main problems are that the local search isn't very good and that the convergence ratio is slow. In 1976, Dawkin came up with the Memetic algorithm, which is based on his notations. The Memetic algorithm is similar to the Genetic algorithm, except that memes are used instead of chromosomes. The main difference in the Memetic algorithm is that the chromosome and its offspring use the local search to get some experience before the evolution process starts. The researchers did their part to make SFLA work better, but there is still more room for performance improvement. In multipath routing, there are more than one way to send a packet from its source to its destination. The congestion management tools will control the flow of packets and the paths. In the past few years, a lot of researchers have worked to improve the performance of complex mechanisms that are based on biological algorithms. Through the exchange of HELLO and TC packets, each node keeps a routing table with entries for nodes from clusters that are up to three hops away from the source cluster. Using HELLO and Cluster Topology Control (CTC) packets, CLSR keeps track of routing information for neighbours up to two hops away. CTC packets are sent out into the network by the CHs. CTC packets are bigger than regular TC packets because they contain information about the source cluster, the members of the source cluster, the information about the neighbouring clusters, and the distance to the neighbouring clusters. For multicast communication to work well, you need to use effective routing techniques. Traffic jams can be avoided with multicast routing, which sends information about the traffic on the roads to the nodes that are about to move to the point in question. This way, the traffic can be redirected to other possible paths. One important thing to keep in mind is to avoid sending packets to nodes that don't need them. This wastes the valuable bandwidth resource. So, the messages need to be sent only to the required nodes using the information about where they are. Geocast routing is one type of routing in VANET. In this type of routing, each node in the network needs to know about itself, such as its location, speed, etc. In geocasting, the source node sends the messages to all the nodes in its area. But these node-based routing protocols don't work well for networks like VANET, where the nodes move quickly and often lose contact with each other because of this. If a node-based routing protocol is used in

VANET, the number of packets that get delivered drops and the amount of work needed to find new routes goes up. So, road-based protocols are put in place to help make the paths more stable. security The method of symmetric cryptography is further developed so that it can provide the services of privacy and can't be changed. For the messages to be encrypted, the Diffie-Hellman key exchange protocol is used to come up with pair-wise session keys. So that the key exchange process can't be attacked, the parameters needed to make the session keys are sent out using their digital signatures to prove that they are real. HMAC-based mechanisms are used to protect the privacy of communications between vehicles and RSUs, between vehicles in the same group, and between vehicles that are not part of a group. Several ways to communicate with a group have been shown. Since the nodes use group signatures to talk to each other, the identities of the nodes are not shared outside of the group. In case of disagreements, the group leader has the power to call and name the original signer. The biggest problems with these approaches are making groups and choosing their leaders. These problems are made worse by the fact that the network topology is always changing. To get around these problems, a new protocol is made that uses group signcryption, which is a combination of group signature and symmetric encryption[18]. According to this protocol, a vehicle that wants to send a message using a group key would first signcrypt the message and then send it on behalf of the sending group to the designated receiving group. Members of the receiving group are the only ones who can decrypt the message by using the group's secret key. So that security needs and handoff performance can be met, the authors have come up with a lightweight authentication scheme. Also, all the access points are split up into different groups. A mobile vehicle chooses an access point, like a base station, and then authenticates itself with the access point. After this kind of authentication is done successfully, the relevant group session key and temporary pair-wise keys are made. The pair-wise transient key is used by the vehicle to talk to the nodes that are close to it[19]. A temporary session key is made when the vehicle switches to a different point of access, especially if that point is in a different group. But if the new point of access is in the same group, no extra steps are needed to finish the authentication process. Using the mechanism of proxy signature, a framework has been made so that RSU can send messages in a safe way. Most of the time, RSUs sign safety messages on behalf of the person who wrote them. The RSUs use proxy re-encryption to send the trusted authority's master key to all nearby nodes. The trusted authority, in turn, gives each vehicle a real name, a set of credentials, and the keys that go with those credentials. Every credential has a number and the trusted authority's signature on the number. The trusted authority saves the mapping of the real identity of the vehicle and the credential numbers that are given to it. This information can be used and shown if there is a dispute about the identity of the vehicle. There are two kinds of messages: those that need to be read right away and those that can wait. The vehicles use the hash-based message authentication code to check that the regular messages are correct (HMAC). But the RSUs need to check the urgent messages to make sure they are true. In this method, the infrastructure or RSUs are used to check each urgent message. Even when it comes to regular.messages, RSUs involve at least some checking of the messages. A solution that uses both the periods of silence and the group signature to protect privacy uses both the Regions and the group signature. In each vehicle, the storage overhead can be kept to a minimum by having the RSUs generate anonymous short-term key certificates as they pass by, based on requests from the vehicle for such certificates. For short-term authentication, these anonymous keys and certificates are used to exchange messages. They have been approved by the certificate authority, which gives the vehicles permission to make their own keys and certificates[20]. The RSUs make it possible to renew the permission every so often. Before the messages are sent, the vehicles attach their own self-made public key to them. An authorised receiver checks the self-generated public keys and the signature on the message to make sure they are correct. During the process of communication, each message has an overhead certificate. This method also uses shared pairs of public and private keys to provide anonymity and verify the identity of an entity. At least one of the sender's active shared private keys needs to be used to sign the message[21-25].

3. Proposed Model

In the proposed work, a large numbers of vehicles are initialized with dynamic network topology. In the initialization process, each node is initialized with random distribution for data communication process. Let V-1,V-2,V-3…Vn represent the vehicles ID in the initialization process. These nodes are initialized with randomized data for the network communication process as shown in figure1.



Proposed Model

Figure 1: Proposed Framework

Figure 1, describes the overall framework of the proposed model. In this framework, all the vehicle nodes are initialized with unique IDs along the network properties. In the dynamic network topology, each node is dynamically initialized with required properties for the communication process. Since the structure of dynamic network topology changes with time, it is difficult to find the route using the traditional models due to static trust computational measures. In this work, node to node link reliability probability is computed to find the trust nodes in the communication process. Here, these trust probabilities are used to group the vehicles based on the threshold. Finally, an optimal Ant Colony Optimization(ACO) model is designed to find the dynamical optimal path planning in the VANET.

Let $V = \{v1, v2..vn\}$ be the $n-$vehicle's list.
The link between any two nodes in the network topology
is given as L(V(i),V(j)).
Let v be the velocity of the vehicle at time t which follows uniformly
normal distribution.
The existence of link between any two nodes in the network at time t
is given as E(l,t).

Step 1: Initialize nodes dynamically in the network.

Step 2: Select k-clusters as initial centers as cluster heads.

Step 3: To each node in the K-cluster heads.

Compute node degree , node velocity and node distance based on the communication range.

$$\text{Node degree } N(D_i) : T_i(R) / V_M(C_j) \quad \text{if } T_i(R) <= V_M(C_j)$$
$$N(D_i) : 1 \quad \text{if } T_i(R) > V_M(C_j)$$

where $T_i(R)$: Total number of nodes within the communication range R of ith vehicle.
$V_M(C_j)$: Total number of maximum vehicles within the each jth cluster.

$$\text{Node Distance } N\left(L(v_i, v_j)\right) : (\log(\| p_{xi} - (\sum_{j \in T_i(R), i != j} p_{xj} / \max\{T_i(R), T_j(R)\}) \| + | p_{yi} - (\sum_{j \in T_i(R), i != j} p_{yj} / \max\{T_i(R), T_j(R$$

R : Communication Radius; (p_{xi}, p_{xi}) : ith vehicle position.

The mean variation between the ith vehicle to jth vehicle in terms of velocity in the given range R

$$\text{VariationVelocity } \Delta\left(V\right) : \| v_i - \sum_{j \in T_i(R), j != i} v_j / \max\{T_i(R), T_j(R)\} \| / \sum_{j \in T_i(R), j != i} v_i / \max\{T_i(R), T_j(R)\}$$

Group the k-clusters based on the node distance and mean variation between the ith cluster head node to jth nodes within the communication range and node degree.

Step 4: Compute node trust and integrity to each neighbor node in the k-cluster head as

if(ND(N_K,nn(i))<R)

Node Trust(N_K,nn(i))

The probablity of link reliabity is computed by using the uniformly normal density function as

$$\kappa = \int_t f(E(l,T))\,dt \;\text{ if } E(l,T) > 0$$

Here, $f(E(l,T))$ is the probability density function over period T .

$$f(E(l,T)) = \frac{R_c(v(i), v(j))}{N\left(D_i\right).\sqrt{2.\Pi\Delta\left(V\right)}} \exp(-\frac{\{R_c(v(i), v(j)) - \Delta\left(V\right)\}}{2.\min\{N\left(L(v_i, v_j)\right)\}}$$

Node integrity: MD5(Data(i))

Step 5: Process all the clusters to the ACO approach for optimal path construction process.

2.Improved ACO for optimal path construction

2.Improved ACO for optimal path construction

Optimized ACO algorithm

Step1:Initialization of ACO parameters

Step 2: To each ant in the number of ants

repeat

Initialize all ant solutions as true

Construct neighbour nodes and its paths until best solutions.

Compute Node pheromone as

Alpha: Pheromone weight

Beta: heuristic wight

$$NPh = Min(Max\_Ph, Max(Min\_Ph, Ph_c))$$

Ph_c : Current pheromone value

NH=1/distance(sn,nn);

$$D(snode, neignode) = \log|(snode.x - neignode.x)^2 + (snode.y - neignode.y)^2|$$

$$Newnode(\alpha, \beta) = N_c.getPh(neig)^{\sqrt{\alpha}} * N_c.getH(neig)^{\sqrt{\beta}}$$

Trust probability is computed to each node for cluster head selection as

$Ph_\alpha = Pheromone\_weight$

$He_\beta = Heuristic\_weight$

Integrated node trust probability for node selection is given as

$$ITP = Ph(N_c)^{\sqrt{Ph_\alpha}} * He(N_c)^{\sqrt{He_\beta}} / \eta * \kappa$$

Where Ph(N$_c$) is the current node's neighbour pheromone and He(N$_c$) is the current node's neighbour heuristic.

Step 3: Update ant local and global best as.

$$\omega = ((1 + (1 - \eta) * (1 - P_c) * H_c) * P_c$$

$$\eta \in (0,1)$$

$$LocalUpdate : (1 - \eta) * (P_n) + \eta * \omega$$

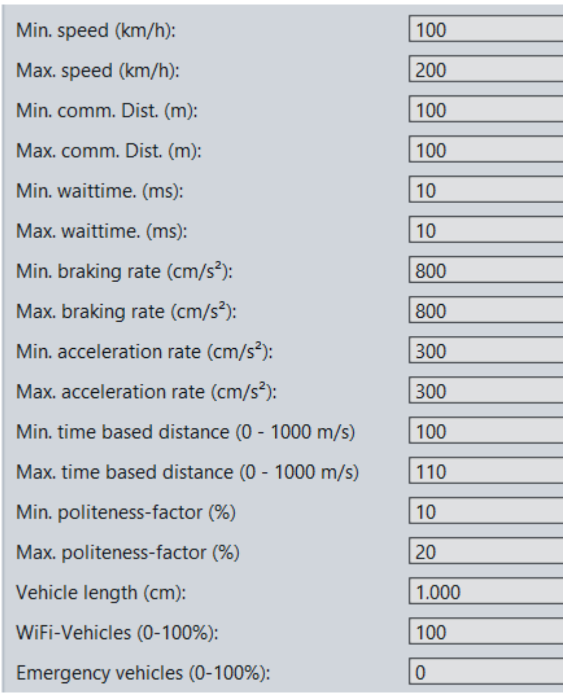
$$GlobalUpdate : (1 - \rho) * (P_n) + \rho * (1 + P_n * H_n) P_n$$

Repeat to each node in the network.

Step 4: dynamic network topology is created with trusted paths.

4.Experimental Results

Experimental results are evaluated on different nodes with different topological structures using java based VANET simulation tool. Experimental results are simulated with different configuration parameters in order to evaluate the performance of the proposed model on the dynamic topology network. Table 1, illustrates the different properties of vehicles and its configuration during the dynamic network initialization process.



Min. speed (km/h):	100
Max. speed (km/h):	200
Min. comm. Dist. (m):	100
Max. comm. Dist. (m):	100
Min. waittime. (ms):	10
Max. waittime. (ms):	10
Min. braking rate (cm/s²):	800
Max. braking rate (cm/s²):	800
Min. acceleration rate (cm/s²):	300
Max. acceleration rate (cm/s²):	300
Min. time based distance (0 - 1000 m/s)	100
Max. time based distance (0 - 1000 m/s)	110
Min. politeness-factor (%)	10
Max. politeness-factor (%)	20
Vehicle length (cm):	1.000
WiFi-Vehicles (0-100%):	100
Emergency vehicles (0-100%):	0

Table 1:Vehicle configuration in the dynamic topology construction

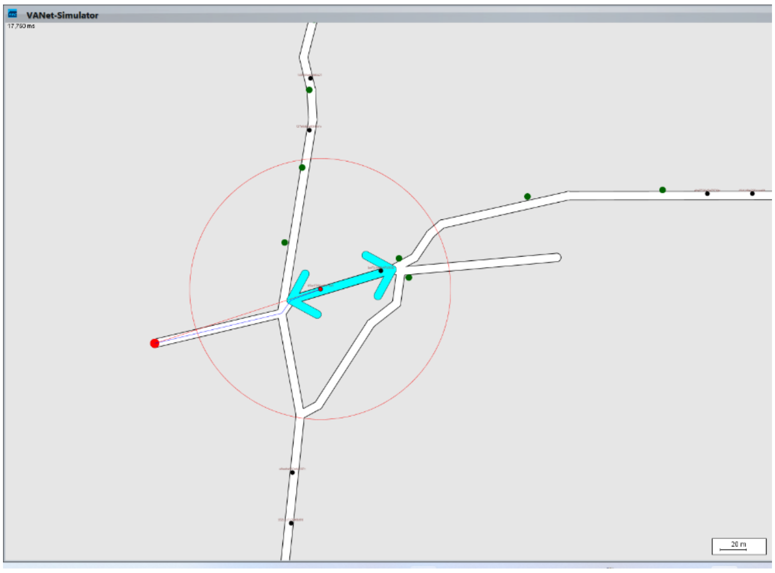


Figure 2: Dynamic network construction with 100 nodes at time t =1

Figure 2, describes the network initialization with 100 nodes at time t=1. As shown in the figure, each vehicle's path is constructed using the proposed algorithm in order to improve the network trustiness and efficient routing process. As shown in the figure, a realtime geographical map is loaded to find the efficient solution of dynamic network construction.

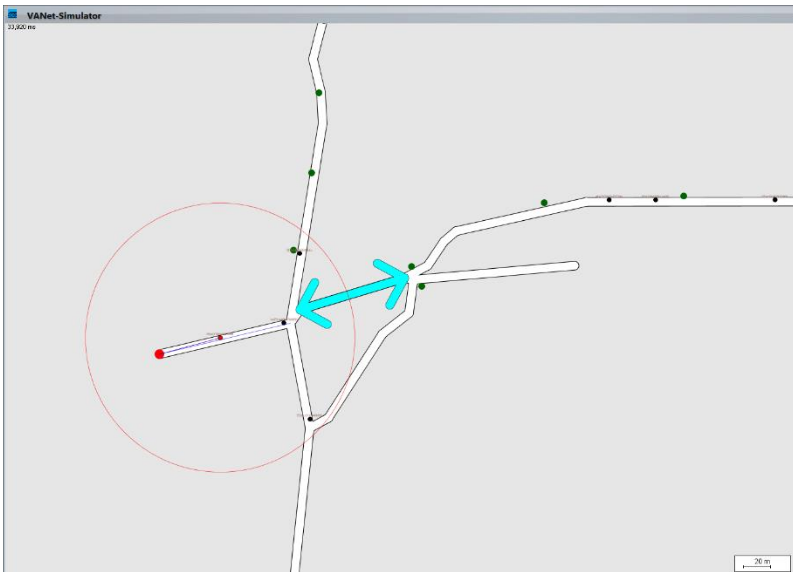


Figure 3: Optimal ACO based path construction with cluster head communication in communication range R

Figure 3, describes the network initialization with 100 nodes at time t=2. As shown in the figure, each vehicle’s path is constructed using the proposed algorithm in order to improve the network trustiness and efficient routing process. As shown in the figure, a realtime geographical map is loaded to find the efficient solution of dynamic network construction.

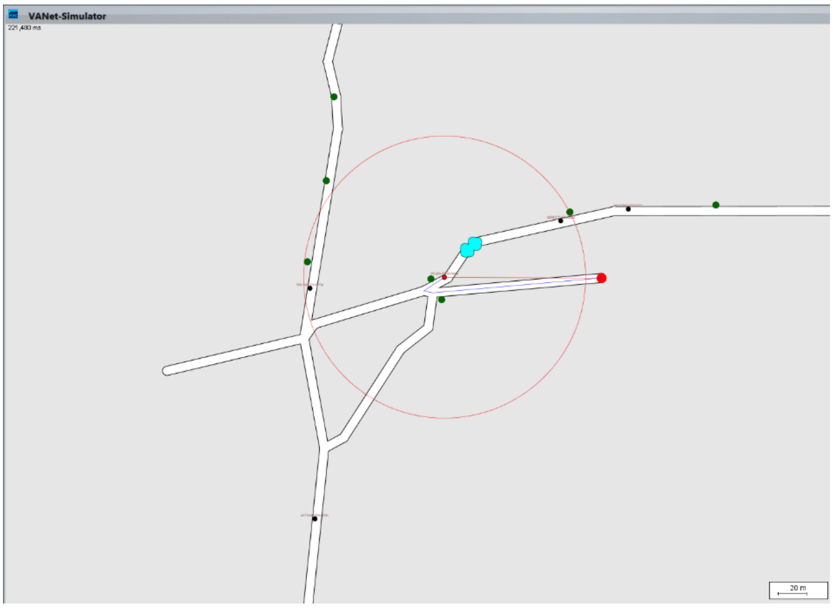
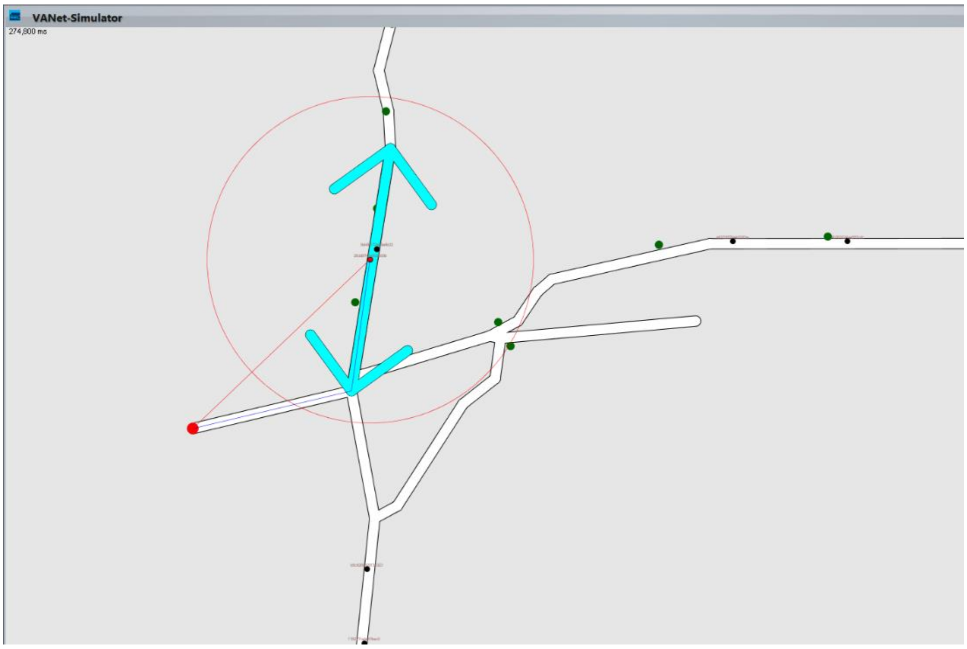


Figure 4: Dynamic network construction with 100 nodes at time t=3

Figure 4, describes the network initialization with 100 nodes at time t=2. As shown in the figure, each vehicle’s path is constructed using the proposed algorithm in order to improve the network trustiness and efficient routing process. As shown in the figure, a realtime geographical map is loaded to find the efficient solution of dynamic network construction.



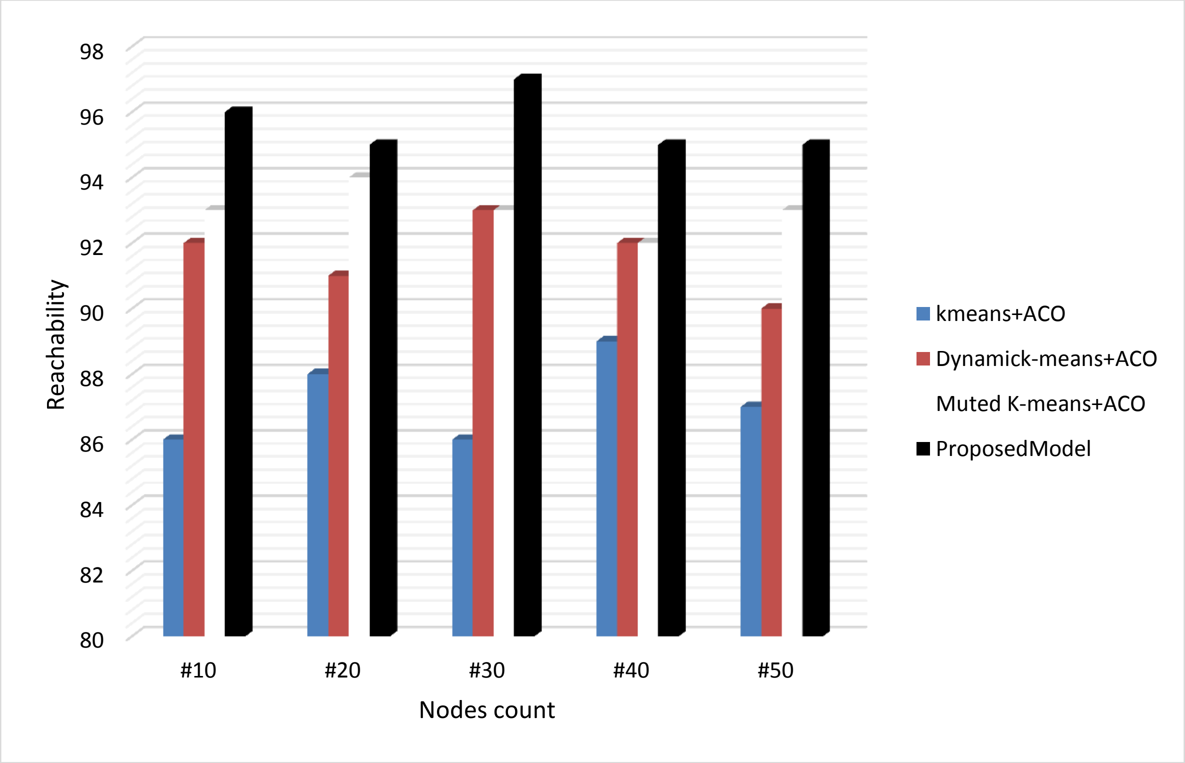


Figure 5: Comparative analysis of proposed node trust based path planning throughput (Kbps) to the conventional models on different VANET networks.

Figure 5 describes the efficiency of proposed link to link trust based path planning throughput to the conventional models on different VANETs. From the figure, it is noted that the proposed model has better throughput than the conventional models for different VANET simulations.

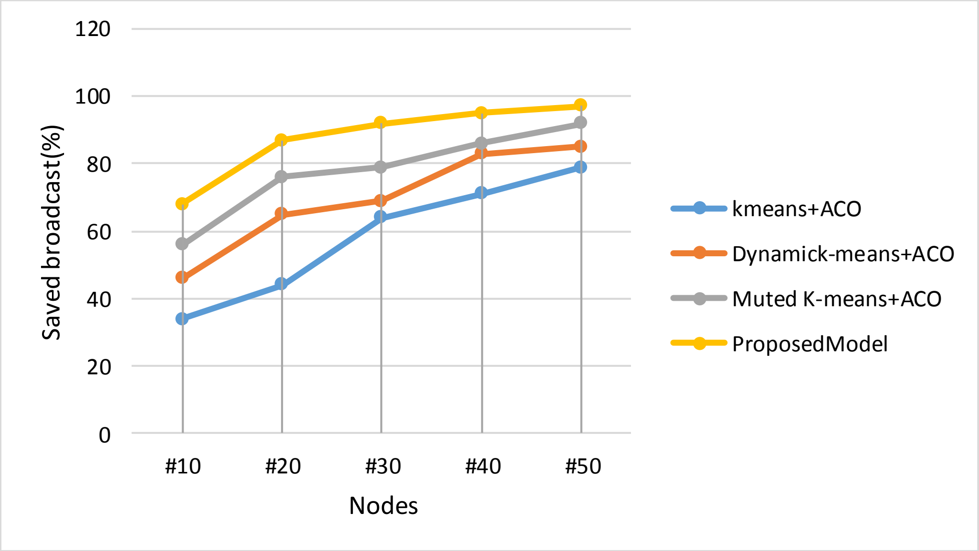


Figure 6: Comparative analysis of proposed node trust based path planning throughput (Kbps) to the conventional models on different VANET networks.

Figure 6 describes the efficiency of proposed link to link trust based path planning throughput to the conventional models on different VANETs. From the figure, it is noted that the proposed model has better throughput than the conventional models for different VANET simulations.

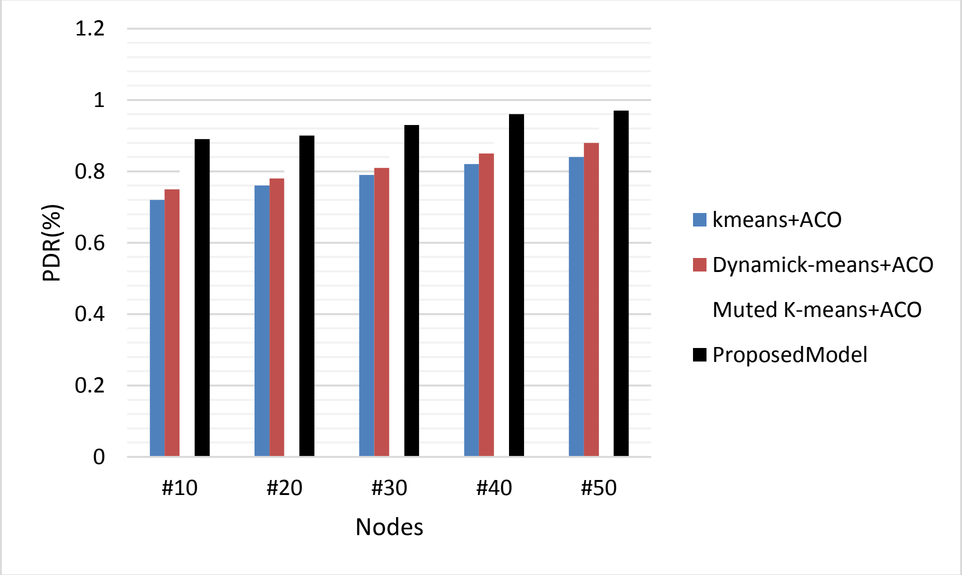


Figure 6: Comparative analysis of proposed link trust node based path planning model to the conventional models on dynamic VANET topology using PDR measure.

Figure 6 illustrates the performance analysis of proposed approach to the conventional models in terms of packet delivery ratio in the dynamic VANET topology. From the figure, it is noted that the proposed model has better PDR than the conventional models.

Conclusion

In this work, a hybrid trust based link estimation and path construction is developed in the VANET. Since, most of the conventional models are difficult to predict the trust , link and path construction during the nodes communication, it is necessary to optimize the trust based dynamic path construction process in real-time applications. Experimental results proved that the present model has better efficiency in terms of PDR, delay and throughput are concerned. Also, in the intra clustering variation, as the number of cluster members are increasing in size, it is difficult create dynamic clusters based on the network topology. In order to overcome these issues, a hybrid VANET clustering framework is implemented based on node properties and trust values. Experimental results show that the present model has better efficiency than the traditional models.

References

[1]I. T. Abdel-Halim, H. M. A. Fahmy, and A. M. Bahaa-El Din, "Mobility prediction-based efficient clustering scheme for connected and automated vehicles in VANETs," Computer Networks, vol. 150, pp. 217–233, Feb. 2019, doi: 10.1016/j.comnet.2018.12.016.

[2]H. Abualola and H. Otrok, "Stable coalitions for urban-VANET: A hedonic game approach," Vehicular Communications, vol. 30, p. 100355, Aug. 2021, doi: 10.1016/j.vehcom.2021.100355.

[3]I. Ahmad et al., "VANET–LTE based heterogeneous vehicular clustering for driving assistance and route planning applications," Computer Networks, vol. 145, pp. 128–140, Nov. 2018, doi: 10.1016/j.comnet.2018.08.018.

[4]B. Alaya and L. Sellami, "Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks," Journal of Information Security and Applications, vol. 58, p. 102779, May 2021, doi: 10.1016/j.jisa.2021.102779.

[5]Y. Allouche and M. Segal, "Cluster-Based Beaconing Process for VANET," Vehicular Communications, vol. 2, no. 2, pp. 80–94, Apr. 2015, doi: 10.1016/j.vehcom.2015.03.001.

[6]X. Bao, H. Li, G. Zhao, L. Chang, J. Zhou, and Y. Li, "Efficient clustering V2V routing based on PSO in VANETs," Measurement, vol. 152, p. 107306, Feb. 2020, doi: 10.1016/j.measurement.2019.107306.

[7]K. Bylykbashi, D. Elmazi, K. Matsuo, M. Ikeda, and L. Barolli, "Effect of security and trustworthiness for a fuzzy cluster management system in VANETs," Cognitive Systems Research, vol. 55, pp. 153–163, Jun. 2019, doi: 10.1016/j.cogsys.2019.01.008.

[8]B. Elira, K. P. Keerthana, and K. Balaji, "Clustering scheme and destination aware context based routing protocol for VANET," International Journal of Intelligent Networks, vol. 2, pp. 148–155, Jan. 2021, doi: 10.1016/j.ijin.2021.09.006.

[9]H. Fatemidokht and M. Kuchaki Rafsanjani, "QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks," Journal of Systems and Software, vol. 165, p. 110561, Jul. 2020, doi: 10.1016/j.jss.2020.110561.

[10]M. S. Kakkasageri and S. S. Manvi, "Multiagent driven dynamic clustering of vehicles in VANETs," Journal of Network and Computer Applications, vol. 35, no. 6, pp. 1771–1780, Nov. 2012, doi: 10.1016/j.jnca.2012.07.002.

[11]R. Kaur, R. K. Ramachandran, R. Doss, and L. Pan, "The importance of selecting clustering parameters in VANETs: A survey," Computer Science Review, vol. 40, p. 100392, May 2021, doi: 10.1016/j.cosrev.2021.100392.

[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,” Vehicular Communications, vol. 13, pp. 78–88, Jul. 2018, doi: 10.1016/j.vehcom.2018.05.002.

[13]P. M. et al., “A Novel Secured Multi-Access Edge Computing based VANET with Neuro fuzzy systems based Blockchain Framework,” Computer Communications, May 2022, doi: 10.1016/j.comcom.2022.05.014.

[14]A. Mchergui, T. Moulahi, and S. Zeadally, “Survey on Artificial Intelligence (AI) techniques for Vehicular Ad-hoc Networks (VANETs),” Vehicular Communications, vol. 34, p. 100403, Apr. 2022, doi: 10.1016/j.vehcom.2021.100403.

[15]K. Ozera, K. Bylykbashi, Y. Liu, and L. Barolli, “A fuzzy-based approach for cluster management in VANETs: Performance evaluation for two fuzzy-based systems,” Internet of Things, vol. 3–4, pp. 120–133, Oct. 2018, doi: 10.1016/j.iot.2018.09.011.

[16]M. L. M. Peixoto et al., “A traffic data clustering framework based on fog computing for VANETs,” Vehicular Communications, vol. 31, p. 100370, Oct. 2021, doi: 10.1016/j.vehcom.2021.100370.

[17]M. Ramalingam and R. Thangarajan, “Mutated k-means algorithm for dynamic clustering to perform effective and intelligent broadcasting in medical surveillance using selective reliable broadcast protocol in VANET,” Computer Communications, vol. 150, pp. 563–568, Jan. 2020, doi: 10.1016/j.comcom.2019.11.023.

[18]M. Ren, L. Khoukhi, H. Labiod, J. Zhang, and V. Vèque, “A mobility-based scheme for dynamic clustering in vehicular ad-hoc networks (VANETs),” Vehicular Communications, vol. 9, pp. 233–241, Jul. 2017, doi: 10.1016/j.vehcom.2016.12.003.

[19]L. Sellami and B. Alaya, “SAMNET: Self-adaptative multi-kernel clustering algorithm for urban VANETs,” Vehicular Communications, vol. 29, p. 100332, Jun. 2021, doi: 10.1016/j.vehcom.2021.100332.

[20]O. Senouci, Z. Aliouat, and S. Harous, “MCA-V2I: A Multi-hop Clustering Approach over Vehicle-to-Internet communication for improving VANETs performances,” Future Generation Computer Systems, vol. 96, pp. 309–323, Jul. 2019, doi: 10.1016/j.future.2019.02.024.

[21]S. Sharma and A. Kaul, “Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET,” Vehicular Communications, vol. 12, pp. 23–38, Apr. 2018, doi: 10.1016/j.vehcom.2017.12.003.

[22]P. K. Shrivastava and L. K. Vishwamitra, “Comparative analysis of proactive and reactive routing protocols in VANET environment,” Measurement: Sensors, vol. 16, p. 100051, Aug. 2021, doi: 10.1016/j.measen.2021.100051.

[23]M. B. Taha, C. Talhi, and H. Ould-Slimanec, “A Cluster of CP-ABE Microservices for VANET,” Procedia Computer Science, vol. 155, pp. 441–448, Jan. 2019, doi: 10.1016/j.procs.2019.08.061.

[24]A. Touil and F. Ghadi, “Efficient dissemination based on passive approach and dynamic clustering for VANET,” Procedia Computer Science, vol. 127, pp. 369–378, Jan. 2018, doi: 10.1016/j.procs.2018.01.134.

[25]O. A. Wahab, H. Otrok, and A. Mourad, “VANET QoS-OLSR: QoS-based clustering protocol for Vehicular Ad hoc Networks,” Computer Communications, vol. 36, no. 13, pp. 1422–1435, Jul. 2013, doi: 10.1016/j.comcom.2013.07.003.