Hindawi
Journal of Engineering
Volume 2020, Article ID 8505280, 12 pages
https://doi.org/10.1155/2020/8505280

Research Article

TAD-HOC Routing Protocol for Efficient VANET and Infrastructure-Oriented Communication Network

Ranjit Sadakale,[1] **N. V. K. Ramesh**,[2] **and Rajendrakumar Patil**[3]

[1]*Dept. of E & TC Engg, Govt. COE, Pune, India*
[2]*Dept. of ECE, K L University, Vijayawada, India*
[3]*Dept. of E & TC Engg, Govt. COER Avasari, Pune, India*

Correspondence should be addressed to Rajendrakumar Patil; rap.extc@coep.ac.in

Received 19 March 2020; Accepted 5 June 2020; Published 13 July 2020

Academic Editor: René Yamapi

Intelligent Transportation System (ITS) is a critical factor for Vehicular Ad hoc Networks (VANET). Even though VANET belongs to the class of Mobile Ad hoc Network (MANET), none of the MANET routing protocol applies to VANET. VANET network is dynamic, due to increased vehicle speed and mobility. Vehicle mobility of VANET affects conventional routing algorithm performance, which deals with the dynamicity of the network node. The evaluation of the existing research stated that Ad hoc On-Demand Distance Vector (AODV) is an effective MANET protocol to adopt network changes for significant resource utilization and also provides effective adaptation in the network change. Due to the effective performance of the AODV protocol, it is considered as an effective routing protocol for VANET. This paper proposed an ad hoc TROPHY (TAD-HOC) routing protocol for the VANET network for increasing efficiency and effective resource utilization of the network. To improve the overall performance, ad hoc network is combined with Trustworthy VANET ROuting with grouP autHentication keYs (TROPHY) protocol. The proposed TAD-HOC protocol transmits data based on time demand in the VANET network with the desired authentication. Results of the proposed approach show the increased performance of the VANET network with packet delay, transmission range, and end-to-end delay. The comparative analysis of the proposed approach with I-AODV, AODV-R, and AODV-L shows that the proposed TAD-HOC exhibited effective performance.

1. Introduction

Vehicular Ad hoc Networks (VANETs) belongs to the class of ad hoc network that inherits Mobile Ad hoc network characteristics (MANETs) with a fewer change in performance [1, 2]. The VANET offers wireless communication through a connection of hundreds or thousands of nodes. In VANET network, On-Board Units (OBUs) are placed nearer to the road, which are a tiny device connected in the VANET network. VANET network contains capabilities of wired communication equipped with road side units (RSUs). In recent years, there is a vast increase in the research domain of MANET, which is composed of singular nature and requirement characteristics [3]. To obtain a specific characteristics solution for VANET, an environment-specific architecture known as Wireless Access in Vehicular Environment (WAVE) architecture is developed [4, 5]. A further variety of safety applications are adopted intrinsically in the VANET network for human-lives saving. Moreover, VANET supports the nonsafety applications, such as contextualized information reception and interactive entertainment applications to interact through the internet or communication with others, such as web sharing and file sharing [6, 7].

VANET routing strategies support vehicle communication in a unicast manner among vehicles for a longer constraint period time [8]. The routing technique in VANET needs to support IP connectivity with an appropriate security strategy for VANET protection. Routing in VANET requires a unique technique for the processing, which does not support the existing handshake-based authentication protocol. VANET requires effective routing and security

mechanisms to withstand secrecy, integrity, and availability for maintaining an effective solution to the environment [9]. Routing and system performance of VANET is widely adopted by WAVE architecture for interdependent and complementary in a network [10, 11]. For effective VANET performance, the IEEE 1609.2 standard involves inefficient performance to secure messages [12, 13].

In a legitimate traffic environment, symmetric cryptography and network authentication involve constraints management. Several management issues are developed through network-wide authentication key factors at the use of specific time for the prevention of cryptanalysis for offering a desirable solution for one or more VUs compromise factor. To overcome this existing drawback in VANET network, Trustworthy VANET ROuting with grouP autHentication keYs (TROPHY) is developed. TROPHY is a protocol set to manage authentication key distribution in VANET VUs [1]. TROPHY protocol design is a mixture with TROPHY message and existing VANET piggyback TROPHY message. VANET environment with OBUs' connectivity (other technologies) is complemented for an ad hoc network solution.

In this paper, we proposed the TAD-HOC routing protocol design for VANET. The proposed architecture combines ad hoc and TROPHY protocol applied in WAVE architecture for the effective performance of the routing network. The primary step involved in this paper is the construction of a VANET network that transmits data in an ad hoc manner. A highway located in Guindy is selected for the evaluation of the proposed network protocol design. SUMO simulation software is used for the construction of a VANET network. The performance of the proposed network is evaluated for various vehicle densities, such as 20, 40, 60, 80, and 100, to measure the packet delivery ratio, network efficiency, network loss, and hoping count. The comparative analysis of the proposed approach with I-AODV, AODV-R, and AODV-L shows that the proposed TAD-HOC exhibited effective performance. The newly proposed routing protocol for the VANET network TAD-HOC is improving the efficiency of the network for efficient resource deployment. TAD-HOC protocol transmits data based on time demand in the VANET network with the desired authentication. The main contributions of this paper are the following:

(i) Review of existing protocols for VANET and comparison with the new proposed TAD-HOC routing protocol

(ii) Performance analysis of the proposed TAD-HOC network, which helps increase the performance of the VANET network with packet delay, transmission range, and end-to-end delay

1.1. Related Work. Wave architecture of IEEE 1609.2 [6] standard provides secure message transmission in the same network environment through the Elliptic Curve Digital Signature Algorithm (ECDSA) asymmetric signature authentication scheme [14]. ECDSA uses a routing message signature with a limited number of the processed message. The signature of this technique adopts behavior in a nondeterministic manner with more than one routing message between a group of mobile nodes with contextual dependencies. ECDSA approach has a limitation of asymmetric primitives, which is not associated with the IEEE 1609.2 standard; it rather adopts a Public Key Infrastructure (PKI), which is mentioned in the existing literature [6, 15]. Vehicular Unit (VU) does not adopt any asymmetric primitives for key exchange; it rather uses PKI instead of the Key Distribution Center (KDC). Authentication in ECDSA uses a set of procedures for the exchange of messages in VUs. In VANET network, VUs are a powerful machine with sporadically distinct characters that do not support any critical signature characteristics. The prosess in a sparse period time is used for appropriate validation of the VUs signature scheme.

In the case of broadcast authentication, the existing work in [16, 17] developed an asymmetric solution mechanism scheme for key disclosure and successive processing with undetermined period time. A developed technique first transmits the message to MAC and it discloses to start another new key. Through the received message from a sender in later stages, the receiver can validate MAC. With the assumption of synchronization, sender and receiver can ensure the key disclosure procedure without any valid key characteristics with the creation of the MAC layer. These factors can be applied in a specific network environment, such as VANET and Wireless Sensor Network (WSN) [18, 19], but they are able to adapt to the routing strategy. In [20], a technique based on time-related constraints characteristics to remove digital asymmetric signature scheme for WAVE architecture was proposed. In this technique, each device requires storing the large number of keys with storing the same key size and device size in VANET. Further precomputed value chain resulted in a one-way function, where all devices are loaded in the network periodically through a new chain and starting chain point to other devices. In such cases, the smaller key count is stored in each device without any periodic, synchronized, and global resetups in all VANET devices.

VANET environment for the smaller area is presented with the solution through a geographical division of regions. The selected regions are recursive into a smaller area with time-related constraints. The proposed approach uses a digital asymmetric signature in WAVE architecture. which follows selected OBUs instruction for registration and delivery of key correspondence and certificates in entering the area. For effective performance, message authentication is speeding up through high priority emergency messages or small area communication [21, 22]. In this way, it is identified that VANET network with a distribution of new cryptographic material has a significant performance. A smaller geographical location with virtual independent character has a virtual group performance in the entire region with symmetric key performance. The geographical area evaluation for the VANET network depends on time and authenticated routing message key which varies from time to time. The key distribution scheme prevents cryptanalysis with symmetric nature of key with proper

cryptanalysis without exclusion of any devices. To explore efficient VANET and infrastructure oriented communication networks, the authors proposed a new TAD-HOC routing protocol. To improve the overall performance of the network in terms of packet delay, transmission range, and end-to-end delay, the proposed TAD-HOC protocol provides an effective solution. We did a comparative analysis of the proposed approach with I-AODV, AODV-R, and AODV-L.

2. Background of Research

VANET network belongs to the category of an ad hoc network environment, which is composed of vast distinct vehicles, such as trucks, buses, motorcycles, and cars. This VANET network is subjected to vast topology changes and increased node mobility [4, 15]. In this VANET network, nodes are considered as vehicles along with the roadside unit. VANET network key and communication issues are due to the high mobility of nodes. Hence, in VANET, it is important to consider network connectivity and routing efficiency with the characterization of link disconnection and change in a network topology. Routing and network connectivity are evaluated for traffic frequency, such as density, demographic variable, and mobility, due to the dynamic behavior of the network. This network is intrinsically associated with the human-lives saving of safety applications [23]. Besides VANET safety application, non-safety applications [24] are also adopted for contextualized information sharing between passengers and entertainment applications for interaction through the internet or among other devices [9, 25].

For a long run time, unicast communication routing strategies are being considered for the VANET application, which critically supports IP connectivity [13, 26]. VANET security is considered as essential parameters. In a routing context, conventional techniques handshake-based authentication protocols [27] are not applicable; hence, a desired solution to security mechanism is required. VANET security mechanism includes integrity, data availability, and secrecy, which does not have any solution at a wider range [28, 29]. Further VANET requires disseminating information at a wider range for roadside interaction for the specific geographical area.

2.1. Organization of Paper. This paper is organized as follows: Section 2 includes context for VANET, where routing protocols work. Section 3 provides proposed TAD-HOC routing strategies. Section 4 describes the architecture of the TAD-HOC routing protocol. Section 5 describes the test scenarios and the corresponding results. The conclusions are in Section 6.

2.2. Preliminaries. VANET routing protocol offers guaranteed information exchange between two nodes. The routing protocol for VANET includes route establishment procedure, forward decision-making process, and recovery of failure nodes. Conventional unicast routing protocol for VANET focused on node duplication and overhead for single packet data transmission in the destination node. As explained earlier, VANET belongs to the class of MANET with unique characteristics routing protocol procedure.

Ad hoc network routing strategy in VANET has several implementation challenges different than the MANET network [6]. Existing Service-Based layer-2 Routing Protocol (SB2RP) is employed in VANET with increased challenges count, which relies on V2I and V2V communication with an appropriate IP address and multihoping in the direct or indirect form [19]. VANET application associated with WAVE is based on the data link layer of the Open Systems Interconnection (OSI) model. In this, a routing algorithm based on distance vector is applied for information routing in infrastructure and VANET communication connectivity [20]. Through IP routing, table information is accessed in the VANET network with Provider Service Identifier (PSID) and information broadcast with WAVE Short Message Protocol (WSMP) for 100 milliseconds. In this paper, we have used routing information for TROPHY authentication exchanged with VU in an auxiliary table. Upon the reception of the message, existing information is replaced with new information. Auxiliary table information is removed and replaced with a period time of 1.5 seconds with three neighboring hops for one second of storage information. VU information offers IP address through possible identification of relationships between variables. VANET routing protocol provides guaranteed exchange between nodes. Routing of VANET involves decision making, establishment, and failed node recovery. Providing optimal path between network nodes via minimum overhead is the key objective for routing protocol.

3. Procedure for the Proposed TAD-HOC

The primary step involved in routing protocol design for the TAD-HOC network environment is the development of the VANET network with appropriate information exchange. Information exchange in the ad hoc network is performed through three types of messages for node controlling with identification and maintenance. AODV network adopts three procedures for information transmission between nodes such as Route Request (RREQ), Route Error (RRER), and Route Reply (RREP) [3]. The performance of each stage is explained as follows, and the overall mechanism is presented in Figure 1:

3.1. Route Request Procedure. The primary mechanism involved in AODV routing is the identification of routes for information packet delivery from source to destination, shown in Figure 2. Each node broadcasts RREQ message to nearby nodes, and neighbor node broadcasts information to the same nearby nodes. This process continues until the destination node is identified for unicast information transmission.

3.2. Route Reply Procedure. If any neighbor node listens to this query and has a destination route to the destination node, it will reply with a route reply packet; otherwise, the

Mechanism of AODV

(1) Initialization of VANETS with the random deployment of vehicles.
(2) Initiate data transmission between nodes with consideration of the sender. In this each node demand path for predefined locations.
(3) Now aggregation of the roadside unit for different vehicular node demands and accessing accepted route information based on time.
(4) Evaluation of nearby node to identify sender and receiver with identification of the shortest path.
(5) Establishment of data communication with transmission and reception of information.
(6) Evaluation of parameters for data communication
(7) Establishment of data communication with transmission and reception of information.
(8) Evaluation of parameters for data communication
(9) End

Figure 1: Mechanism of AODV [3].

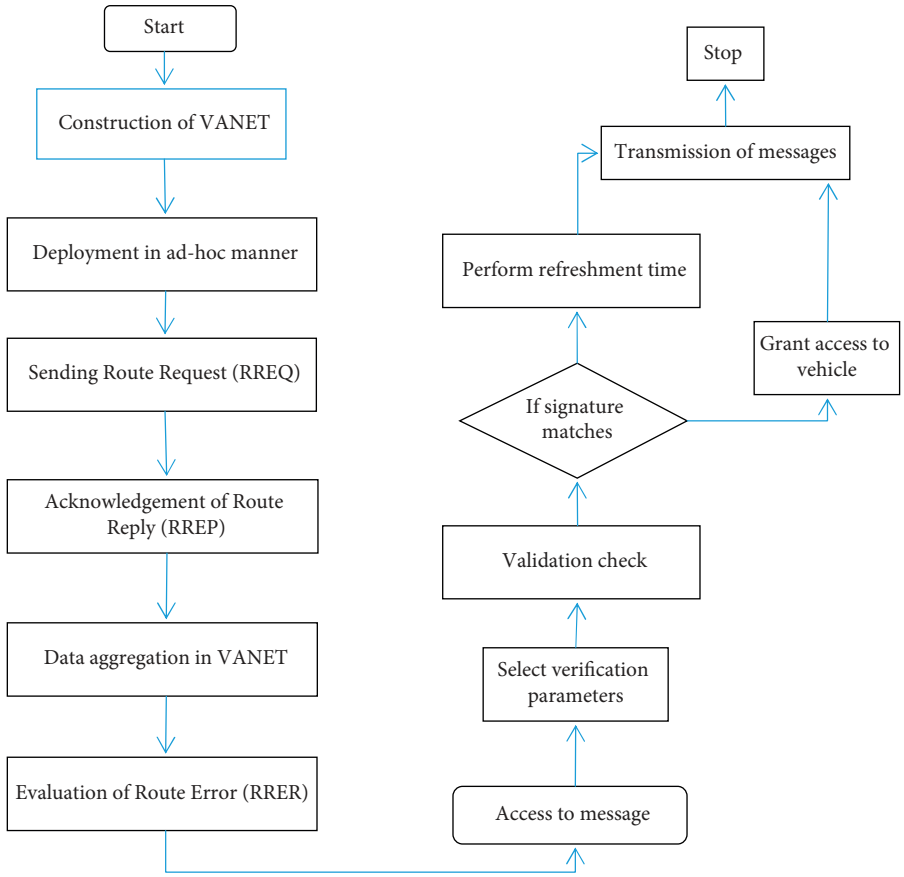

Figure 2: Flowchart for AODV mechanism.

neighbors rebroadcast the route query packet, until it reaches its destination. When the RREP message is received, the route is established. RREP can be received multiple times by a source node with a different route to the destination. The routing table only will be updated if the RREP has a greater sequence number.

3.3. Route Maintenance Procedure. A node is identified with the generation of error message or breakage of inactive route. For recovering this node information, RRER message is transmitted to neighboring or destination node as shown in Figure 3. Upon reception of the RRER message, the IP address of the node is retrieved from the routing table and alternately broadcasts RREP message. After reception of RREQ message from node 1, its neighbor starts replying with RREP message or rebroadcasts RREQ message to its neighbors. The node starts transmitting RREP message if the routes to destination are evaluated. The messages keep transmitting until the message lifespan continues. In case that node 1 did not receive any reply at the specified set of times, it starts rebroadcasting RREQ messages with the ID number. Every node in the network uses a set of the sequence number for RREQ with insured properties:

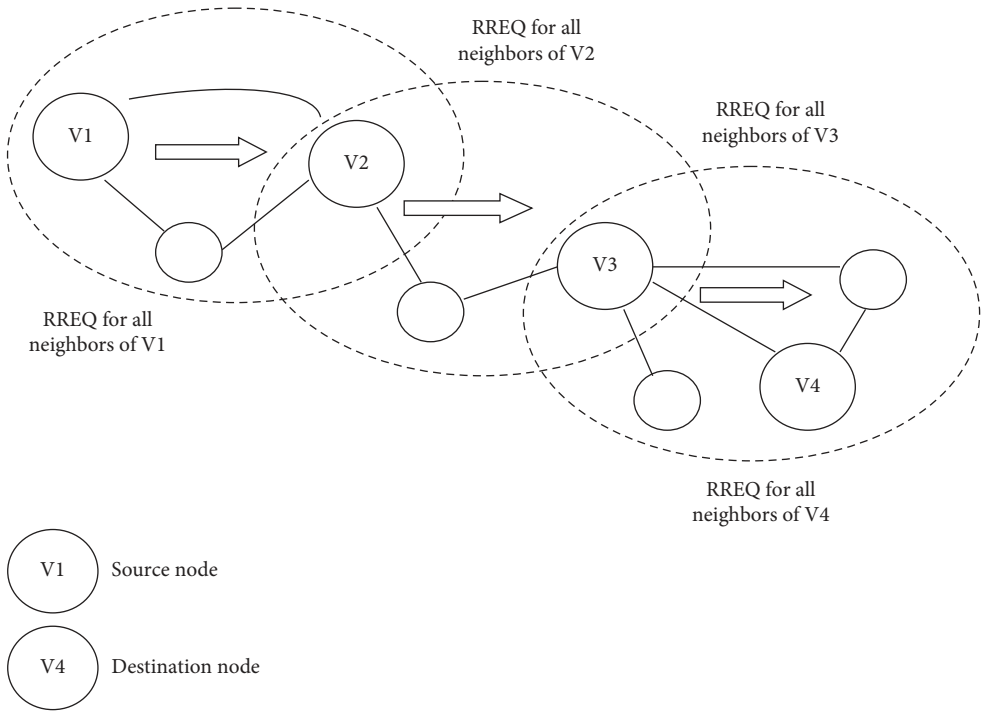

Figure 3: Transmission of RREQ in AODV.

$$R(\text{RREQ}) = \sum_{n-1}^{H} (4)3^{(H-1)} \sum_{i=2}^{4} \left[(n-1-i) - \sum_{j=1}^{H-1} N_j \right] p^{Ci}, \tag{1}$$

where C_i is the additional coverage index of a node that has i, neighbors, H is the number of hops of the network, and N_j is the number of neighbors at the hop.

3.4. Proposed TAD-HOC Routing Protocol. In this paper, we have proposed a TAD-HOC routing protocol for the VANET network, which is presented in Figure 4. In the proposed approach, routing messages are transmitted between vehicles that allow transmission of the message to neighboring nodes. TROPHY is used to route information to vehicles for authentication. Based on time demand, routing information is protected through patented routing information. Proposed TAD-HOC adopts SB2RP. In the proposed TAD-HOC approach, authorized nodes sequentially receive TROPHY messages, which allow them to retain cryptographic material and keep authentication keys updated across the network. Messages of the TAD-HOC network epidemically presented throughout the network are not able to perform the refreshment using them (and so, are excluded from the routing process). In TAD-HOC, KDC is stored for the recovery of messages through unauthorized physical access without human intervention.

Developed TAD-HOC architecture contains four entities, such as OBUs, RSUs, KDC, and human operator. OBUs and RSUs are considered a single entity. Also, KDC is responsible for message creation, update, and periodic distribution of messages for network routing authentication. KDC communicates with a human operator for setup and update of network operation. In the analysis, the routing key is generated in MAC, which is shared between all VUs denoted as ρ. Refreshment interval and routing key parameters were mentioned as ρ with a sequence of values $\rho(1), \rho(2), \rho(3), \ldots, \rho(t-1), \rho(t), \rho(t+1)$.

3.4.1. Interaction between Entities. The human operator can include or exclude new VUs at any time and it reconfigures some network-wide parameters in the KDC. The routing process is initiated on those VUs, after the initial setup by the human operator [1]. The routing messages exchanged between VUs, known as beacons, are authenticated with a MAC. To anticipate its potential, the routing key is periodically refreshed by the KDC. Also, if one or more VUs are pinpointed as lost or physically compromised, the human operator can immediately launch a key refreshment to prevent the exploitation of a possible leaked routing key [1]. The refreshment process is also used to exclude the compromised VUs after that from the VANET's routing (the VUs to exclude are not involved in the key refreshment process).

When we mention ρ, we mention the routing key without taking into consideration specific refreshments associated with a time interval [1]. The multiple refreshments of ρ create a sequence of values identifiable as $\rho(1), \rho(2), \rho(3), \ldots, \rho(t-1), \rho(t), \rho(t+1)$. Ad hoc architecture with VANET is controlled through KDC at a specified time interval with regular updates. KDC time interval was associated with real-time processing with a different duration of time. In the ad hoc network, recent index has been used for VU in VANET with a message

Mechanism of TAD-HOC
Sender node
(1) Initialization of VUs in VANET
(2) Calculate time interval 't' to evaluate node present status
(3) Encrypt KDC public key for auxiliary key calculation α
(4) Compute the last exclusive key of MAC through previously computed content
(5) Computation of MAC last routing key with the previous content
Receiver node
(6) Identification of VUs in VANET
(7) Encryption of subset value of nodes
(5) Encryption based on the time interval
(6) Sends information control message
(7) Signature authentication in KDC
(8) Acknowledgment of messages
(9) End

Figure 4: Mechanism for TAD-HOC.

update of the period $\rho(t)$ associated with the $t+1$ circulated VANET network. VUs based on timestamp well-defined KDC period are updated. For an arbitrary update, VUs are updated with a time stamp, which is not desirable. The presence of an absolute period is involved in effective decision making of routing with minimal clock synchronization of VUs.

Based on ad hoc routing TROPHY network nodes have a different version. To validate routing key, VUs use various routing key version to validate MAC. Routing information is updated through Beacon signal to compute MAC validation at the receiver denoted as ρ. MAC Beacons are used for computation of ρ for triggering and neighbor update. In each VU, recent ρ is created and verified based on IP routing packet information exchange.

3.4.2. Key Refreshments. In the proposed network, refreshment of a key is considered a major factor for transmission and reception of messages in the network. Refreshment update r(t) is performed with a refreshment parameter ρ in VANET key information of VUs with correspondent public key signature validation with preloaded value. Refreshment update r(t) along with auxiliary information processes asymmetric cryptography in the network [21]. At a specified time interval, "t" refreshment messages are associated with RSUs. To receive new messages, RSUs and KDC periodically communicate with OBUs redistribution Beacon signal.

Epidemic key refreshment is processed through VUs with cryptographic material in state "t" and the previous network state is defined as $(t-1)$. In the chained process of data transmission to refresh different keys, refreshment message is used at the same time on various VUs without breaking the secrecy. VANET symmetric key uses ρ for isolation MAC Beacons for neighbor's key reception.

4. Architecture of TAD-HOC

The proposed TAD-HOC platform with TROPHY architecture is influenced by a trade-off in multiple scenarios with acceptable cost, complexity, and overhead with the introduction of efficient policies and protocol layers with effectiveness correspondingly [30, 31]. Generally, the VANET network is the interconnection of a thousand devices with minimizing individual intervention at each time in devices with restriction of associated action with other devices. Routing protocol for real-time performance requires effective protocol operation and aligned hardware availability with limitation of asymmetric cryptography primitives. Based on this, the developed ad hoc VANET architecture uses group identity in a shared manner. Group identity in a shared manner will not recognize each other; rather, it involves global identity. The share group key identity categorizes authorized and unauthorized members within the group, for exploring authentication between group members based on primitives of symmetric cryptography.

The exposure of proposed network architecture captures network attacks to minimize network loss. Identity control groups consider members either individually or in subgroups. In this scenario, the proposed architecture design contains an entity in either a unique or centralized manner to retain KDC responsibility. The group identity of each member evaluated identity based on control and stores group identity. KDC involvement in proposed architecture increases the security of stored data in the network for new information transmission among each member of the network. On the other hand, VANET global state information exchange offers fast information exchange of data with guaranteed ad hoc infrastructure requirement specifically for the solution to cellular network [32].

The mechanism for TAD-HOC is explained in Figure 5. Assume that the ad hoc network environment does not offer a desirable solution to information transmission at a faster rate. Hence in the proposed TAD-HOC network, environment epidemic propagation mechanism is adopted [28]. Through this developed epidemic approach, VANET members receive new information based on best effort policy members without any mutual trust among members. Authentication is performed with an exchange of authenticated messages among member groups with KDC sign contents.

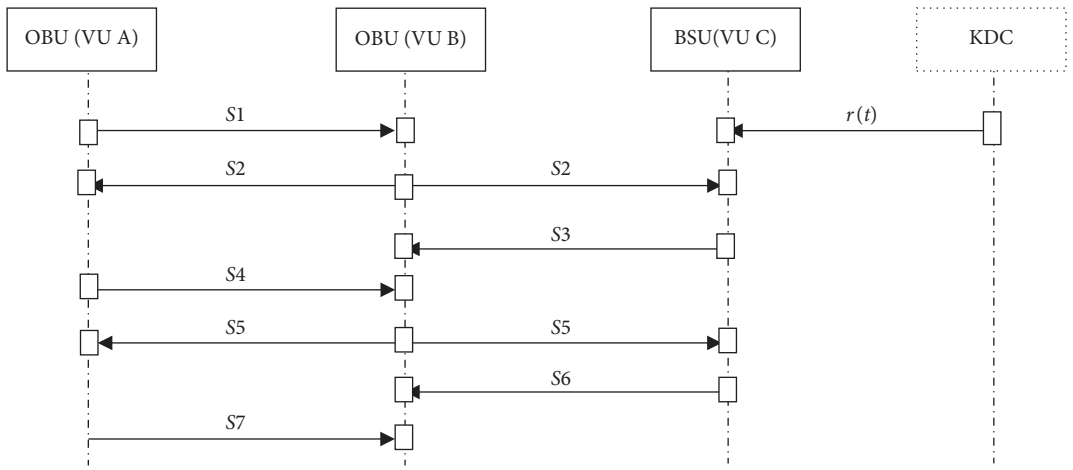

Figure 5: Refreshment time of TAD-HOC.

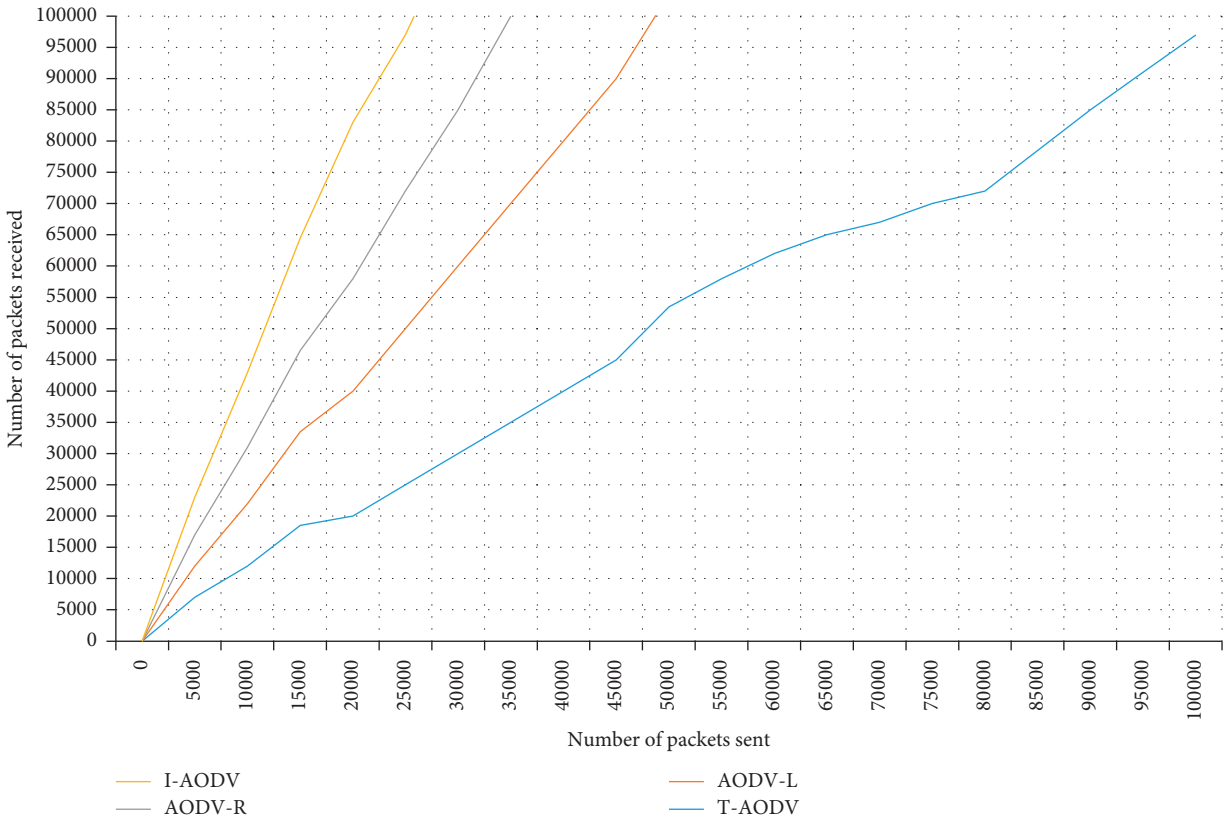

Figure 6: Packet delivery ratio of the network.

The policy infrastructure of the authenticated group involves global computational resources and bandwidth consumption policy information [22, 29]. Symmetric cryptography key reduces the consumption of computational resources that functions with the impact of asymmetric cryptography members which are dynamic.

4.1. Proposed TAD-HOC Algorithm. AODV is simply a routing mechanism to transmit information between different network devices. This mechanism transmits information among the VANET network where the nodes cannot communicate directly. In Figure 6, we have considered the deployed ad hoc network with three nodes for communication between each other. Through the limitation of mobile nodes, each communicates to a nearby node for effective data transmission. In the proposed scenario, node X communicates with node Y which may be a nearby node directly. This node keeps a record of neighboring nodes at a set of specified interval time. Node X transmits a HELLO message to node Y. Suppose one node transmits information to another node which is not a neighbor; then that node

sends RREQ message. This RREQ message contains information with several key bits of information data such as source, destination, sequence number, and message lifespan with a unique ID. Assume that node 1 is expected to send a message to node 3 where direct communication is not possible. RREQ messages are transmitted to node 3 where node 2 is able to hear the message.

4.2. Simulation Setup. The simulation setup used for evaluating the performance of the proposed TAD-HOC network is presented in Table 1. The proposed TAD-HOC approach is comparatively examined with conventional I-AODV, AODV-R, AODV-L. In a simulation setup for each VANET node, each one is equipped with GPS receivers. Performance of the proposed approach is evaluated in terms of average hop count, end-to-end delay, packet delivery ratio, network energy consumption, network efficiency, and network loss. Simulation is performed for various vehicle densities such as 0, 20, 40, 60, 80, and 100.

In the simulation, the proposed TAD-HOC network VANET is deployed on the highway selected in Guindy. This entire VANET network design is based on an urban scenario. SUMO simulation is used for designing ad hoc network design for selected highway in Guindy. In highways, Guindy occupies topmost position due to major vehicle involvement in the VANET. Hence, we selected Guindy highway for evaluation of the proposed TAD-HOC network. So in a simulation, it is considered as a proper area for handling and bounding the simulation results. The simulation time is 300 msec, and six simulations are done for each protocol. The simulation setting is as mentioned in Table 1.

Table 1: Simulation setting for the proposed TAD-HOC network.

Parameter	Value
Maximum vehicle speed	40 kmph
Transmission rate	0.5 Mbps to 5 Mbps
Transmission range	250 m
Simulation area	Guindy highway
Number of vehicles	0, 20, 40, 60, 80, 100
Simulation time	300 msec

5. Results and Discussion

In this paper, we use a packet delivery ratio, end-to-end delay, and routing overhead for performance analysis.

5.1. Packet Delivery Ratio. Packet Delivery Ratio (PDR) is the contrast factor for PLR. In PDR, the number of packets received in the receiver end is evaluated in terms of the number of the transmitted packet. The effective wireless network needs to have a significant PDR value for effective performance in the network. PDR is calculated as

$$\text{Packet Delivery Ratio} = \frac{S1}{S2}, \tag{2}$$

where $S1$ is the sum of data packets received by each destination and $S2$ is the sum of data packets generated by each source.

PDR for the proposed TAD-HOC is maximal compared with other techniques for various vehicular densities. TAD-HOC exhibits a higher PDR rate of 25.65, 45.24, 62.19, 72.58, and 97.23 for vehicle density 20, 40, 60, 80, and 100. Table 2 shows a comparison of existing technologies such as I-AODV, AODV-R, and AODV-L which provide a minimal PDR compared with the proposed approach.

5.2. End-to-End Delay. End-to-end delay generally describes the duration to send and receive the information packets, which can be successfully received at the destination node. In this paper, the end-to-end delay between source and destination is compared. One of the assumptions made is that the nodes have dynamic mobility. This assumption supported different scenarios, such as overtaking scenarios and also out of bounding scenarios, and hence was able to predict the location of neighbors shortly which reduced end-to-end delays:

$$\text{delay} = \left(D_{\text{proc}} + D_{\text{queue}} + D_{\text{trans}} + D_{\text{prob}}\right)\left[\frac{d}{Tx}\right], \tag{3}$$

where, D_{proc} is the processing delay, D_{queue} is the queuing delay, D_{trans} is the transmitting delay, D_{prob} is the propagation delay, and d/Tx is the number of hops between the sender and receiver.

The end-to-end delay of the TAD-HOC network provides minimal delay compared with existing techniques which is illustrated in Figure 7 and Table 3. The TAD-HOC technique offers minimal delay of 125.37 for vehicle density 100. In other techniques, for vehicle density of 40, 60, and 80, a maximum delay of 375.21 in the I-AODV approach was exhibited.

Figure 8 and Table 4 show the average hop count for different networks for sending packets from the source to the destination by predicting the location of neighbors shortly.

In the proposed approach, hoping count is a major factor for performance measure. Hoping involves the overall computation time involved in the network. The measure of hoping clearly stated that the proposed approach has a significant reduction in the hoping count of vehicles. Network with vehicle density of 100 has a hoping value of five which is significantly minimal compared with the conventional technique.

5.3. Efficiency of Network. VANET network with infrastructure oriented requires an effective network structure for communication of vehicles. Hence, the TAD-HOC network is examined for efficiency in terms of energy consumption, packet loss, and energy efficiency of the network. Table 5 represents the overall summary of network efficiency in comparison with I-AODV, AODV-R, and AODV-L.

For various vehicle densities, network efficiency is measured under energy consumption, energy efficiency, and loss. The proposed TAD-HOC network infrastructure has minimal packet loss with increased efficiency of the network. Packet loss of the proposed network is 120 for vehicle count

Table 2: Comparison of PDR for different existing techniques.

Vehicle density	I-AODV	AODV-R	AODV-L	T-AODV
0	0	0	0	0
20	15.45	18.20	20.50	25.65
40	30.20	33.53	38.91	45.24
60	55.70	58.13	60.00	62.19
80	63.25	65.72	70.33	72.58
100	75.85	82.37	89.11	97.23

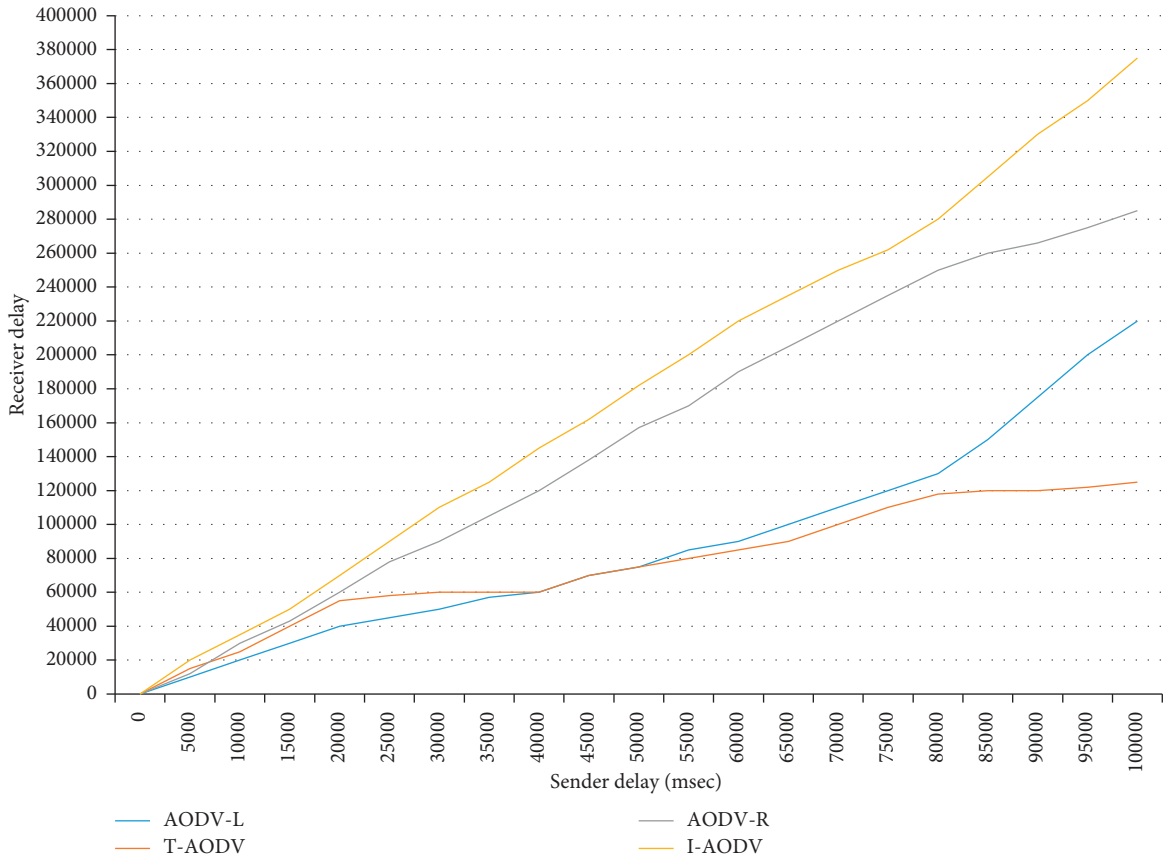

Figure 7: End-to-end delay of network.

Table 3: Comparison of end-to-end delay for different networks.

Vehicle density	I-AODV (msec)	AODV-R (msec)	AODV-L (msec)	T-AODV (msec)
0	0	0	0	0
20	70.47	60.67	40.86	55.20
40	145.83	120.22	60.44	63.63
60	220.35	190.31	90.75	85.91
80	280.87	250.73	128.35	115.40
100	375.21	285.37	220.75	125.37

100, while in examining efficiency, it is observed as 92.37, which is significantly higher than the existing approaches. The energy consumption rate of a proposed protocol for 100 vehicles is 7.63. Through the comparative analysis, it is concluded that the proposed approach is effective compared with the other existing techniques.

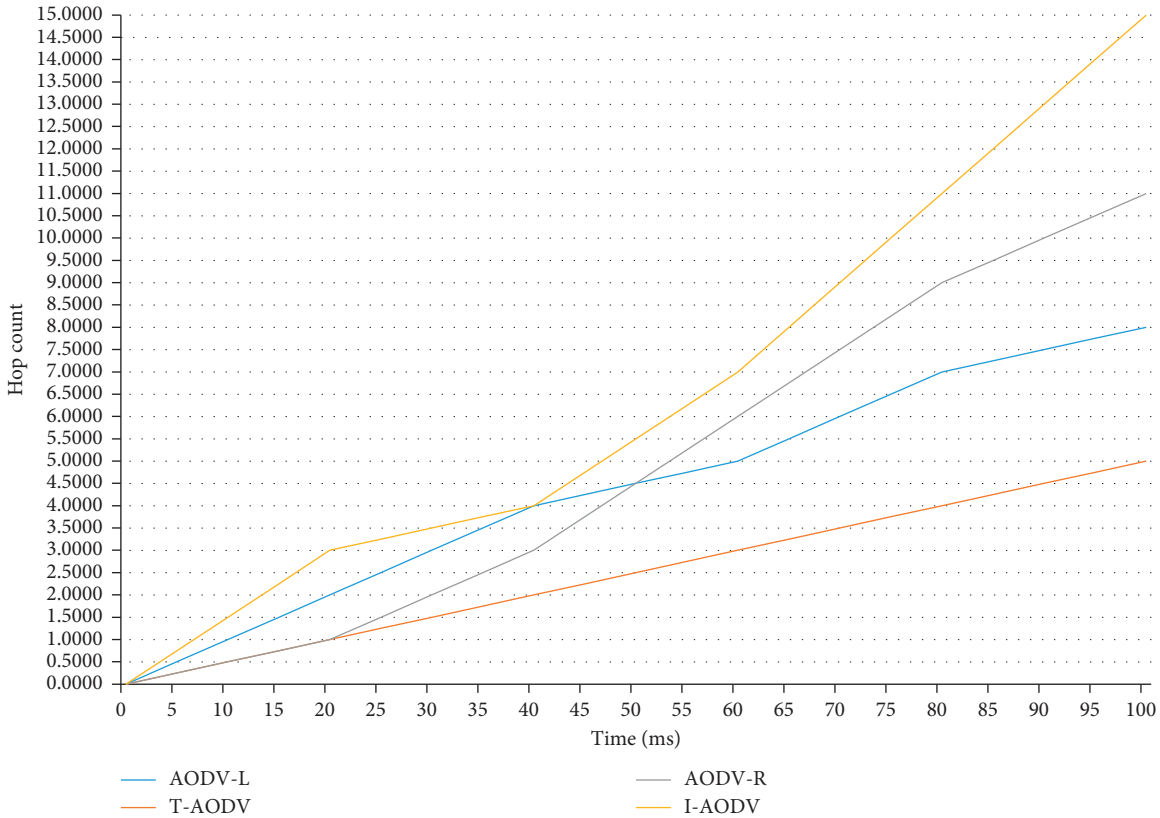

Figure 8: An average hop count of the network.

Table 4: Average hop count for different networks.

Vehicle density	I-AODV	AODV-R	AODV-L	T-AODV
0	0	0	0	0
20	3	1	2	1
40	4	3	4	2
60	7	6	5	3
80	11	9	7	4
100	15	11	8	5

Table 5: Summary of network efficiency of different network.

Vehicle density	I-AODV	AODV-R	AODV-L	T-AODV
Packet loss in network				
0	0	0	0	0
20	125	110	50	15
40	302	205	104	30
60	408	301	175	55
80	480	370	303	75
100	537	423	385	120
Energy consumption of the network				
0	0	0	0	0
20	10.20	7.40	3.21	2.17
40	15.48	13.81	5.35	3.39
60	20.37	17.38	7.55	4.77
80	23.41	20.17	11.30	5.61
100	28.65	24.11	14.17	7.63
Energy efficiency of the network				
0	0	0	0	0
20	15.20	30.45	40.25	55.91
40	22.18	50.85	53.40	65.35
60	40.37	63.77	72.30	80.76
80	65.81	70.40	80.66	85.68
100	71.35	75.99	85.83	92.37

6. Conclusion

VANET network contains capabilities of wired communication equipped with RSUs. To obtain specific characteristics, solution for VANET environment-specific architecture known as WAVE architecture is developed. The VANET routing strategies support vehicle communication in a unicast manner among vehicles for a longer constraint period time. The routing technique in VANET needs to support IP connectivity with an appropriate security strategy for VANET protection. Routing in VANET requires a unique technique for the processing, which does not support the existing handshake-based authentication protocol. VANET requires effective routing and security mechanisms to withstand secrecy, integrity, and availability for maintaining an effective solution to the environment. The proposed TAD-HOC routing protocol for the VANET network is increasing the efficiency of the network for effective resource utilization of the network. TAD-HOC protocol transmits data based on time demand in the VANET network with the desired authentication. The results of the proposed approach increased the performance of the VANET network with packet delay, transmission range, and end-to-end delay. The comparative analysis of the proposed approach with I-AODV, AODV-R, and AODV-L shows that the proposed TAD-HOC exhibited effective performance. In the future, this study can be further improved in the rural and urban scenarios for safety and nonsafety applications.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] P. Cirne, A. Zúquete, and S. Sargento, "Trophy: trustworthy VANET routing with group authentication keys," *Ad Hoc Networks*, vol. 71, pp. 45–67, 2018.

[2] I. Abbasi and A. Shahid Khan, "A Review of vehicle to vehicle communication protocols for VANETs in the urban environment," *Future Internet*, vol. 10, no. 2, p. 14, 2018.

[3] E. Ndashimye, S. K. Ray, and N. I. Sarkar, "-to-Infrastructure communication over multi-tier heterogeneous networks: a survey," *Computer Networks*, vol. 112, pp. 144–166, 2017.

[4] R. G. Gutiérrez, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014.

[5] R. S. Bali, N. Kumar, and J. J. P. C. Rodrigues, "Clustering in vehicular ad hoc networks: taxonomy, challenges and solutions," *Vehicular Communications*, vol. 1, no. 3, pp. 134–152, 2014.

[6] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie, "Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends," *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, Article ID 745303, 2015.

[7] A. Berridge and Z. Mammeri, "Multi-hop broadcasting in VANET for safety applications: Review and classification of protocols," *International Journal of Business Data Communications and Networking*, vol. 9, no. 4, pp. 86–104, 2013.

[8] V. Kumar and S. Mishra, "Applications of VANETs: Present & future," *Communications and Network*, vol. 05, no. 01, pp. 12–15, 2013.

[9] J. Chand, Q. Pan, and Z. He, "VANET middleware for Service sharing based on OSGi," *Computer Science and Information Systems*, vol. 12, no. 2, pp. 729–742, 2015.

[10] M. Oche, A. B. Tambuwal, C. Chemebe, R. M. Noor, and S. Distefano, "VANETs QoS-based routing protocols based on multi-constrained ability to support ITS infotainment services," *Wireless Networks*, vol. 26, no. 3, pp. 1685–1715, 2018.

[11] C. Ghorai and I. Banerjee, "A robust forwarding node selection mechanism for efficient communication in urban VANETs," *Vehicular Communications*, vol. 14, pp. 109–121, 2018.

[12] K. Zhu, D. Niyato, P. Wang, E. Hossain, and D. I. Kim, "Mobility and handoff management in vehicular networks: a survey," *Wireless Communications and Mobile Computing*, vol. 11, no. 4, pp. 459–476, 2011.

[13] D. R. L. Brown, M. J. Campagna, and S. A. Vanstone, "Security of ECQV-certified ECDSA against passive adversaries," *Cryptology ePrint Archive*, http://eprint.iacr.org/2009/620.pdf, 2011.

[14] D. G. Reina, S. L. Toral, F. Barrero, N. Bessis, and E. Asimakopoulou, "The role of ad hoc networks in the Internet of things: a case scenario for smart environments," *Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence*, Springer, Berlin, Germany, pp. 89–113, 2013.

[15] S. Al-Sultan, M. Moath, Al-Doori, A. H. Al- Bayatti, and H. Zedan, "A comprehensive survey on Vehicular Ad Hoc network," *Journal of Network and Computer Applications*, vol. 37, pp. 380–392.

[16] M. Alajeely, R. Doss, and A. a. Ahmad, "Routing protocols in opportunistic networks—a survey," *IETE Technical Review*, vol. 35, no. 4, pp. 369–387, 2018.

[17] J. Alves Junior, C. Emilio, and G. Wille, "Routing in vehicular ad hoc networks: main characteristics and tendencies," *Journal of Computer Networks and Communications*, vol. 2018, Article ID 1302123, 10 pages, 2018.

[18] S.-H. Han, H.-J. Lim, and T.-M. Chung, "The Possibility to resolve the security Problems through the LTE in vehicular ad-hoc networks," *World Academy of Science, Engineering and Technology International Journal of Electronics and Communication Engineering*, vol. 6, no. 4, 2012.

[19] Y. L. Morgan, "Managing DSRC and WAVE standards operations in a V2V scenario," *International Journal of Vehicular Technology*, vol. 2016, Article ID 3261602, 1 pages, 2016.

[20] K. Z. Ghafoor and M. A. Mohammed, "Routing protocols in vehicular ad hoc networks: survey and research challenges," *Network Protocols and Algorithms*, vol. 5, no. 4, 2013.

[21] X. Ji, H. Yu, G. Fan, H. Sun, and L. Chen, "Efficient and reliable cluster-based data transmission for vehicular ad hoc networks," *Mobile Information Systems*, vol. 2018, Article ID 9826782, 15 pages, 2018.

[22] C. Hoe Lee, K. Guan Lim, M. Keng Tan, R. Ka Yin Chin, and K. Tze Kin Teo, "Hybrid simulation network for vehicular ad hoc network (VANET)," *ICTACT Journal on Communication Technology*, vol. 9, no. 1, pp. 1686–1695, 2018.

[23] B. T. Sharef, R. A. Alsaqour, and M. Ismail, "Vehicular communication ad hoc routing protocols: a survey," *Journal*

of Network and Computer Applications, vol. 40, pp. 363–396, 2014.

[24] S. Tajik, G. Farrokhi, and S. Zokaei, "Performance of modified AODV (waiting AODV) protocol in mobile ad-hoc networks," in *Proceedings of the ICUFN 2010*, IEEE, Dalian, China, June 2010.

[25] X. Zeng and Y. Ming, "A new Probabilistic multi-hop broadcast protocol for vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 12165–12176, 2018.

[26] M. Gonzalez-Martín, M. Sepulcre, R. Molina-Masegosa, and J. Gonzalez, "Analytical models of the performance of C-V2X mode 4 vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1155–1166, 2019.

[27] L. Zhao, F. Wang, K. Zheng, and T. Riihonen, "Joint optimization of communication and traffic efficiency in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 2014–2018, 2019.

[28] H. Moustafa and Y. Zhang, *Vehicular Networks: Techniques, Standards, and Applications*, Auerbach Publications, Boca Raton, FL, USA, 2009.

[29] A. Khan Jadoon, L. Wang, Li Tong, and M. Azam Zia, "Lightweight cryptographic techniques for automotive cybersecurity," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 1640167, 15 pages, 2018.

[30] Tao Ming, W. Wei, and S. Huang, "Location-based trustworthy services recommendation in 2 cooperative-communication-enabled Internet of vehicles," *Journal of Network and Computer Applications*, vol. 126, pp. 1–11, 2018.

[31] G. Li, L. Boukhatem, and S. Martin, "An intersection-based WoS routing vehicular ad hoc networks," *Mobile Network Applications*, vol. 20, pp. 268–284, 20105.

[32] D. Das and R. Misra, "Improvised dynamic network connectivity model for Vehicular Ad-Hoc Networks (VANETs)," *Journal of Network and Computer Applications*, vol. 122, pp. 107–114, 2018.