Wireless Personal Communications (2021) 121:2589–2608
https://doi.org/10.1007/s11277-021-08838-w

Energy Efficient Enhanced OLSR Routing Protocol Using Particle Swarm Optimization with Certificate Revocation Scheme for VANET

C. BrijilalRuban[1] · B. Paramasivan[2]

Accepted: 6 August 2021 / Published online: 30 October 2021

Abstract
In Vehicular ad-hoc networks (VANETs), routing and security are the mainchallenges. In our previous work, we have presented cluster-based secure communication with the certificate revocation scheme for securable communication between the vehicles.Cluster formation is done using the trust degree of each vehicle and this trust degree is calculated based on the direct and indirect trust degree of each vehicle. Information of eachvehicle is gathered by the corresponding cluster head (CH) in a cluster. This information is maintained by the Certificate Revocation List (CRL) in the Certificate Authority (CA). CA isolates a vehicle as an attacked node if it has less trust degree than the threshold trust value and it invalidates the certificate of attacked or revoked nodes. Before transmission, each vehicle in a cluster validates its certificate with the support of CA. After the validation, the other challenge of VANET i.e., efficient route is to be established so that Energy efficient enhanced OLSR routing protocol using Particle Swarm Optimization (PSO) algorithm is presented in this paper. After the establishment of the efficient route, the vehicle deploys the symmetric cryptography approach for securable transmission. Simulation results show that the performance of our proposed approach outperforms the performance of existing work in terms of energy efficiency.

Keywords Vehicular ad-hoc networks (VANETs) · Trust degree · Certificate revocation list (CRL) · Certificate authority (CA) · OLSR routing protocol · Particle swarm optimization (PSO) · Symmetric cryptography

✉ C. BrijilalRuban
brijilalruban0301@gmail.com

[1] Anna University, Chennai, Tamilnadu, India

[2] Department of Computer Science and Engineering, National Engineering College, Kovilpatti, Tamilnadu, India

1 Introduction

The vehicular ad-hoc network is generally used to communicate among moving vehicles in a definite atmosphere. Here, Vehicle to Vehicle (V2V) communication is explained about the communication between vehicles directly [1, 2]. Additionally, Vehicle-to-Infrastructure is illustrating about the communication between a vehicle and an infrastructure like a Road Side Unit (RSU) [3, 4]. Normally, the VANET has no predetermined structural design or topology. On the other hand, a common VAN ET is used to communicate between moving vehicles or some nearby RSU. According to this situation, VANET is dissimilar to a MANET, in which, vehicles are not moving arbitrarily like nodes in MANETs, rather than moving vehicles encompass predetermined paths like urban roads and highways. At the same time, it thinks about VANETs as a division of MANETs. Suppose, if it takes in designing of network structural design, then it is significant to consider of VANETs like an entity study area. In VANET structural design, an onboard unit (OBU) includes a wireless transmitter and receiver in a vehicle. Here, we can easily describe three feasible communication circumstances for vehicles. The initial communication is that every vehicle communicates with each other with the help of RSU. This structural design also looks like wireless local area networks (WLAN). The second communication is that vehicles openly communicate with each other and without RSU, which is categorized as Ad-hoc structural design. The third communication is that the combination of both like some vehicles can communicate openly and further need some RSU to communicate [5].

In VANET, security is a significant process to protect further networks in communication. Moreover, the VANETs contain several possible attacks. The foremost intention of attacks is to generate difficulty for consumers to contact the system or stealing the information [6, 7]. In a vehicular network, every application is premeditated to protect the extremely sensitive information from malicious manipulation which is communicated through VANET. Suppose, if it is not detected that the sensitive message is manipulated, and then it will origin the. Additionally, comfort and eminence functions are necessitating protecting from profits failure in VANET. Therefore, our anticipated method contains cluster-related secure communication through a certificate revocation system. In this method, the certificate authority is exploited to authorize the certificate for safe communication.

Moreover, we need an effective routing algorithm to send data packages from one node to another node inappropriate manner [8–11]. Here, an effectual routing algorithm is a routing format among least postponement, greatest system capability, and less computational difficulty. This kind of algorithm is executed in multiple topology networks which is a current study in VANET. Normally, the foremost intention of a routing algorithm is to sense and maintain the finest route to send data packages through intermediate nodes. According to the dynamic mobile nodes, searching and accumulating routes is a difficult process in VANETs. As an extension of our previous work, we present an Energy-efficient enhanced OLSR routing protocol using Particle Swarm Optimization with Certificate Revocation Scheme for VANET. The contribution of our work is described as below,

- As the cluster formation has been presented in our previous work, cluster formation is to be done in this paper.
- Revoked (attacked) nodes are preserved in the Certificate Revocation List (CRL). Before transmission, each node in a cluster verifies the validation of certificate from the Certificate Authority (CA) for secure communication.

- After the verification, the source node forwards the data to the destination by the way of optimal path. This optimal path is to be established based on the enhanced OLSR routing protocol. Multi-point relay (MPR) selection is the major component in OLSR. For optimal MPR selection, Particle Swarm Optimization (PSO) algorithm is presented in this work.
- We simulate this proposed technique on the network simulator NS2.
- Experiments results show that performance of our proposed approach is superior to that of the existing work in terms of energy efficiency.

Rest of this paper is organized as follows. Section 2 surveys some previous literature that focused on the research of routing and security in VANET. Our proposed energy efficientenhanced OLSR routing protocol using Particle Swarm Optimization with Certificate Revocation Scheme for VANET is presented in Sect. 3. Results of our proposed approach are discussed in Sect. 4. This paper is concluded with Sect. 5.

2 Literature Survey

In this section, some previous literature that focused on the research of routing and security in VANET is survived. In VANET, efficient routing is one of the major components to solve the problem of energy efficiency. So, Husain and Sharma [12] have proposed geographical location based routing protocols in VANET. They have implementedtwo geographical routing protocolsbased on IEEE802.11pthat are LAR (location-aided-routing protocol) and ZRP (zone-routingprotocol) to solve the problem of communication breaks between the vehicles. However theperformance of the LARP outperformed the performance of the ZRP, it should be improved in terms of energy efficiency. Similarly, Toutouh et al. [13] have introduced aparallel evolutionary algorithm which has been used to explore for energyefficient OLSR structures. This algorithm outperformed the existing configuration in terms of energy consumption. However, they have not focused on secure transmission. For securable transmission, Ganan et al. [14] have proposed an Efficient and Privacy-Aware revocation Mechanism (EPA). This proposed approach has been performed with the support of a Crowds-based anonymous protocol and Merkle Hash Trees. It replaced the time-consuming certificate revocation lists verifying process. Similarly, Rahbar and Daeinabi [15] have presented an advanced Secure scheme based on Clustering and Key Distribution. This scheme has been executed among cluster-heads and members in VANET. For securable communication, this scheme has deployed proxy signature, message authentication, and symmetric cryptography.However, efficient routing should be combined with the security system to improve the energy efficiency of the network.

Saleh et al. [16] have introduced a Reliable Routing Protocol for VANET. The network has been divided into overlapping zones using this protocol. A special node has been selected as a master node for each zone. This master node maintained the routing boards for inter-zone and intra zone communications. This protocol discovered available routes to the destination and selected the most efficient route among them. Similarly, Bitam et al. [17] have presented a Hybrid Bee swarm Routing (HyBR) protocol in VANET. This protocol combined the properties of geographic routing with those of topology routing. Mirjazaee and Moghim [18] have proposed an innovative opportunistic-based routing algorithm (OSTD) for urban scenarios. This proposed approach has evaluated the efficient routes by calculating the utility function.

Authors also have used the predictability of Vehicle's driving path to transmit the packet. Liu et al. [19] have proposed limited broadcasting by connectivity zones based enhanced AODV routing protocol for data forwarding in large-scale VANET. Authors evaluated the performance of the connectivity zones with the function of grey correlation analysis method.

However theabove-mentioned protocols are improved in terms of delivery ratio and end-to-end delay, theenergy efficiency of the network has to be improved further.

3 Energy Efficient Enhanced OLSR Routing Protocol Using PSO With Certificate Revocation Scheme

3.1 Overview

As an extension of our previous work, Energy efficient enhanced OLSR routing protocol using PSO with Certificate Revocation Scheme for VANET is presented in this paper. Initially, vehicles in the region are grouped into separate clusters. In each cluster, cluster head (CH) is based on the trust degree of the vehicles. The vehicle with lesser trust degree than minimum trust degree or threshold value is identified as the attacked node. List of these attacked or revoked nodes are included in the Certificate Revocation List (CRL). The certificate authority is responsible to maintain the information of CRL.The CA is responsible to revoke and assign the certificates of the vehicle node. The Certificate Authority identifies, if any vehicle involves any malicious activity, immediately it revokes their certificates even before the expiration dates. To direct all the vehicles in the cluster, the certificate authority furnishes valid digital certificate to every CH. All the cluster heads are behave as a mobile repository to store the details about the active nodes (witness nodes) and the ids of the revoked nodes.After the validation of certificates, a vehicle within a cluster transmits its data packet to the corresponding cluster head and the CH sends the gathered data to the base station through the optimal path. This optimal path is selected using our proposed approach which is to be known as PSO based OLSR routing protocol. In this approach, multipoint relay selection (MPRs) that included in OLSR routing protocol is optimized using Particle Swarm Optimization. After the establishment of the optimal path, the data packets will be transmitted by using the symmetric cryptography application, over the selected path. By presenting this enhanced OLSR routing protocol, theenergy efficiency of the network will be improved. Figure 1 shows the block diagram of our proposed approach.

3.2 Cluster Formation

Initially, vehicles in the zone are to be accumulated into different clusters based on trust degree of each vehicle as mentioned in our previous work. Among vehicles ormembers in a cluster, a cluster head (CH) is selected based on the weight of the vehicle. This weight is calculated for each vehicle using the parameters such as number of neighbor vehicles, transmission range, speed of the vehicle and the trust degree. Then the vehicle, which has less weight, is elected as a CH.The weight factor for each vehicle is calculated using the following equation.

$$w_i = \alpha * R_T + \beta * V_{Neigh_i} + \delta * S - \gamma * T_{\deg} \quad (1)$$

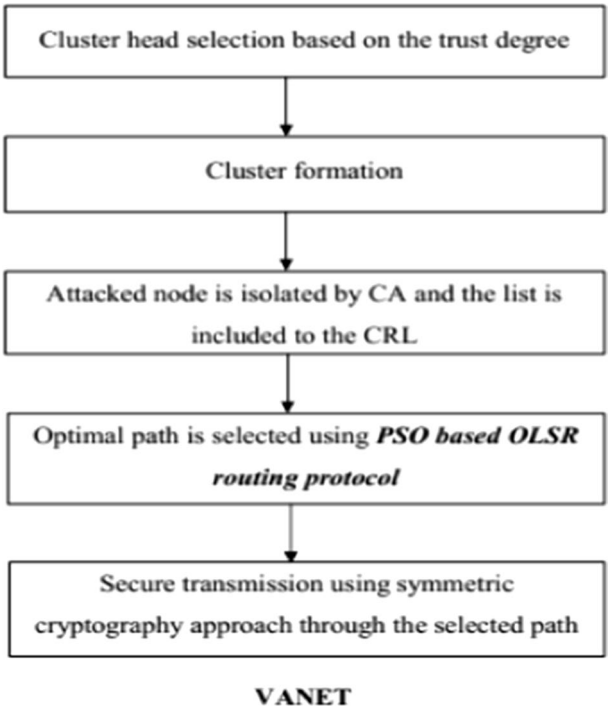

Fig. 1 Block diagram of our proposed approach

where α, β, γ and δ are the constant weights range from 0 to 1. R_T, V_{Neigh_i}, S and $T_{\deg}$ are representedas the transmission range, number of neighbor vehicles, speed of the vehicle, and trust degree of the vehicle respectively.

From the above equation, trust degree is the significant parameter for the selection of CH and for the identification of inactive or attacked node. This trust degree value is calculated using direct trust and indirect trust values. Direct transmission between the sender and receiver node is known as direct trust. Transmission between the sender and receiver node is done with the support of in between trusted vehicle, is known as indirect trust. Direct trust value between the vehicles s and d is calculated using the following equation,

$$T^D_{n+1} = \begin{cases} T^D_n(s,d) + RC, (SC > 0) \\ T^D_n(s,d) + PC, (FC > 0) \end{cases} \tag{2}$$

where T^D_n denotes the previous trust degree that was calculated during the selection of previous CH. RC and PC are known as Reward Coefficient and Punishment Coefficient respectively, those are used to update the similarity between s and d.SC and FC are represented as the number of successful communications and number of unsuccessful communications respectively in the time interval Δt.

Direct trust value between the vehicles s and d is calculated using the following equation

$$T^{\mathrm{ID}}_{(s,d)} = \frac{\sum_{j \in l} S(s,j) * T^D(j,d)}{\sum_{j \in l} S(s,d)} \tag{3}$$

where j represents the neighbor vehicle that is common to both$s$ and d. $S(s, j)$ represents the similarity between the vehicles s and j. l represents the most similar nearest-neighbors of s and d.

Using equations () and (), the trust degree is calculated using the below equation

$$T(s,d) = \eta * T^{D}(s,d) + \mu * T^{\mathrm{ID}}(s,d) \tag{4}$$

where η and μ are represent the weighting factors direct trust degree and indirect trust degree respectively.

Each vehicle calculates the weight value using Eq. (16). Then the vehicle connects to the cluster head, responsible in that region. Thus the cluster is formed as shown in Fig. 2.

3.3 Isolation of Revoked Nodes

After the cluster formation, CH in each cluster receives information message about its non-CH members. This information message includes ID and trust degree of the vehicles. CH forwards these gathered information messageto the Certificate Authority (CA) which is a trusted third party, this authority will generate the signed certificate for requested vehicle. CA maintains the Certificate Revocation List (CRL) which maintains the list of the vehicles and their information. After receiving the information message from the CH, CRL verifies that whether the vehicle is normal or attacked one. If the trust degree of the vehicle is lesser than the threshold trust degree ($T < T_{\mathrm{th}}$),the vehicle is identified as an attacked node.Then CA revokes the certificates of the malicious vehicles before the expired period.It forwards the revoked node ID to the corresponding CH as shown in Fig. 3. The CH forwards that information to all nodes except to the revoked node.After receiving the information from the CH, all nodes verifies their buffer whether the revoked node previously performed any abnormal activity or not.

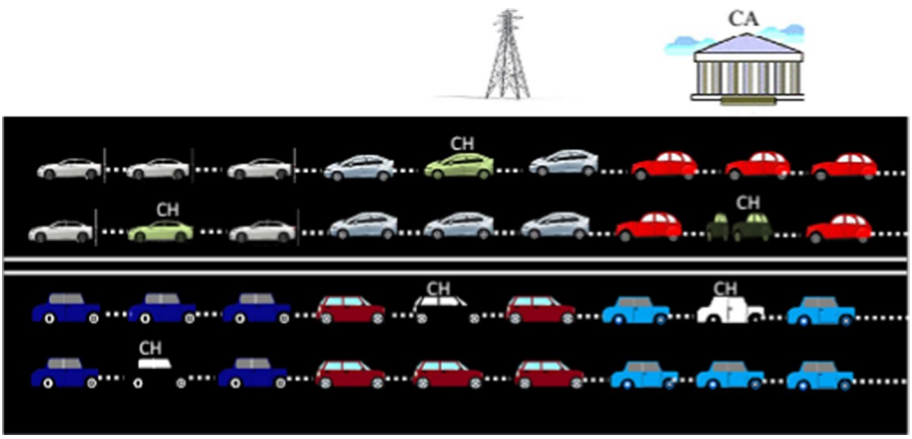

Fig. 2 Cluster heads (CHs) selection

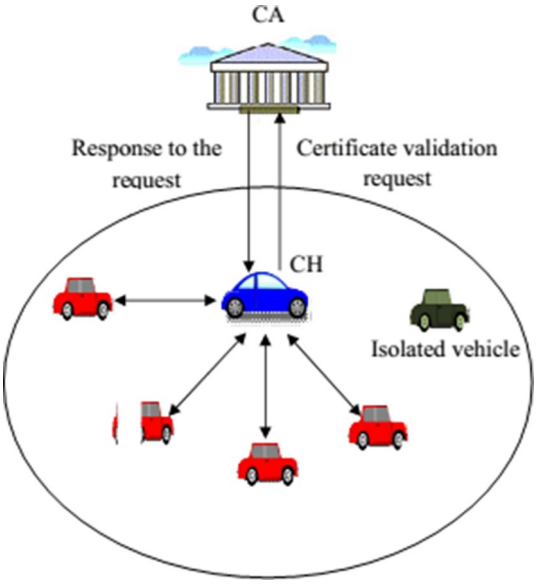

Fig. 3 Communication between CH and CA

3.4 Enhanced OLSR Routing Protocol Using Particle Swarm Optimization

When ever vehicle nodes need any details about its certificate, it can demand its respective cluster. After the collection of certificate details, the vehicle can start the communication only it its certificate is valid. Before transmission, efficient route will be established between the source and base station. For efficient routing, Enhanced OLSR routing protocol using Particle Swarm Optimization is presented.

3.4.1 Overview of OLSR Protocol

Optimized Link State Routing protocol is a proactive LSR protocol.Multi-point relays (MPRs)selection is the major idea of the OLSR protocol. By the selection of these MPRs, information exchange overhead will be reduced in the network. The importance modules of the OLSR are described as follows,

3.4.1.1 Neighbor Sensing In neighbor sensing, each CH forwards HELLO message to its neighbor nodes. This message contains ID of the neighbor nodes and their link status. The nodes located in 1-hop neighborhood of a node will be selected as MPRs. In this way, HELLO messages permit each node to detect its neighbors up to two hops away.

3.4.1.2 Efficient Broadcasting of Control Traffic To control the traffic efficiently, the selected multi point relay nodes only permitted to broadcast the information.

3.4.1.3 Broadcasting Sufficient Topological Information Topology Control (TC)message is the other type of control packets. It is used to broadcast sufficient topological details in the network. This topology control messages are originated by the MPRs to know which other

CHs have chosen it as their MPR. Therefore all the heads of the cluster get some topological view and present the subset of links in the adhocnetwork.This TC message permits each CHto estimate its own routing table.

3.4.2 Proposed Optimal MPR (OMPR) Selection

Multi point relay nodes are responsible to control and forward the traffic details of the network. It is very essential to create the best non-CHs in a cluster as a MPR node because the effectiveness of the OLSR protocol is based on the multi point relay node.To select the optimal MPR nodes form the set of MPRs, Particle Swarm Optimization (PSO) is presented.

Kennedy and Eberhart developed the Particle Swarm Optimization., PSO was influenced by the social response and natural movement of a flock of birds moving towards a common intention like Genetic Algorithm (GA) that imitates the process of natural progression. This algorithm considered the particles are like the swarm of birds as the multi-dimensional problem area and also considered the speed they travel as the velocity of the particles.Optimal MPR selection using this algorithm is presented phase by phase.

3.4.2.1 Initialization Initially, the selected MPR nodes are initialized as the candidate solutions or particles i.e.,

$$P_i = \left[X_{i,1}(t), X_{i,2}(t), \ldots, X_{i,D}(t)\right] \tag{5}$$

where $X_{i,d}(t)$ denotes the position of the ith particle or MPR in the dth dimension. This is also represented as,

$$X_{i,d}(t) = \left(x_{i,d}(t), y_{i,d}(t)\right), \quad 1 \le i \le N_P,\ 1 \le d \le D \tag{6}$$

where N_P denotes the population size of the particles.

3.4.2.2 Fitness Measure From the initialized particles or MPRs, optimal MPRs are selected by measuring fitness value of each MPR. This fitness value is measured using the metrics Residual energy, Link stability and Buffer occupancy of each MPR node. Evaluation of these metrics is described below.

3.4.2.3 Residual Energy Residual energy of each MPR node is calculated as using below equation

$$E_{residual,i} = E_{initial,i} - E_{consumed,i} \tag{7}$$

where $E_{initial,i}$ and $E_{consumed,i}$ are characterized as initial and consumed energy of node i. By scheming the total amount of transmission and reception energy of a node i, energy ingestion of the node is calculated as follows

$$E_{consumed,i} = u_i \times E_T + v_i \times E_R \tag{8}$$

where u_i and v_i are characterized as the number of transmitted bits and received bits in node i. E_T and E_R are characterized as transmission energy and reception energy correspondingly and are calculated as

$$E_T = E_{T_{radio}} + E_A \times dis_{\text{mn}}^2 \tag{9}$$

$$E_R = E_{R_{radio}} \tag{10}$$

where $E_{T_{radio}}$ and $E_{R_{radio}}$ are the energy that the radio requirements for the transmitter and the receiver correspondingly, E_A is signified as the energy of the transmit amplifier and the distance within two nodes *m* and *n* is signified as *dis*.

3.4.2.4 Link Stability Link stability that establishes a route betweentwo nodesand it is calculated as

$$LS = \frac{R}{dis(m,n)} \tag{11}$$

where *R* denotes the transmission range, $dis(m, n)$ between two neighboring nodes.

Finally, Fitness function for selecting optimal MPR is calculated using equation () and () i.e.,

$$Fitness_i = \alpha * E_{residual,i} + \beta * LS_i + \gamma * B_i \tag{12}$$

where α, β and γ are denoted as a weighting factor ranging from 0 to 1. *Bi* denotes the buffer occupancy of *i*th node.The particle with maximum fitness value is our optimal solution to select the OMPR.

3.4.2.5 Updation The direction and velocity will be changed until the particles finally meet at a solution with each creation of motion, The Velocities and locations are explained in PSO as:

$$v_{i+1} = w \cdot v_i + c_1 \cdot r_1 \cdot \left(pbest_i - Y_i\right) + c_2 \cdot r_2\left(gbest_i - Y_i\right) \tag{13}$$

$$Y_{i+1} = v_{i+1} + Y_i \tag{14}$$

where c_1 and c_2 are represented as the self-recognition component coefficient and social component coefficient respectively. These values have same positive constant value. r_1 and r_2 approach for a uniformly distributed random number in the interval (0, 1). *w* is represented as the inertial weight of the particle, which is initialized to 1 and is gradually reduced over time. The value $pbest_i$ is the best position of the particle. $gbest_i$ is the global best value among the *pbesti* value. *Yi* represents a position of *i*th particle in the search area which alters based on updates on *vi* which represents the velocity.

3.4.2.6 Termination When the fitness of particle (P) is greater than the fitnessof *pbest*, then the particle *P* is considered as the *pbest* particle. Otherwise the *pbest* particle is updated using Eqs. (13) and (14). If the fitness of updated *pbest* is better than the fitness of *gbest,* then the updated *pbest* particle is assigned as *gbest* particle. Otherwise the *gbest* particle is updated. This process is repeated until we get the optimal solution or optimal MPR from the initialized MPRs. Once the optimal solution is attained, the algorithm will be terminated.Algorithm for OMPR selection is described below and Fig. 4 shows the flow diagram of this algorithm. Figure 5 shows the selection of optimal MPRs or vehicles in a cluster.

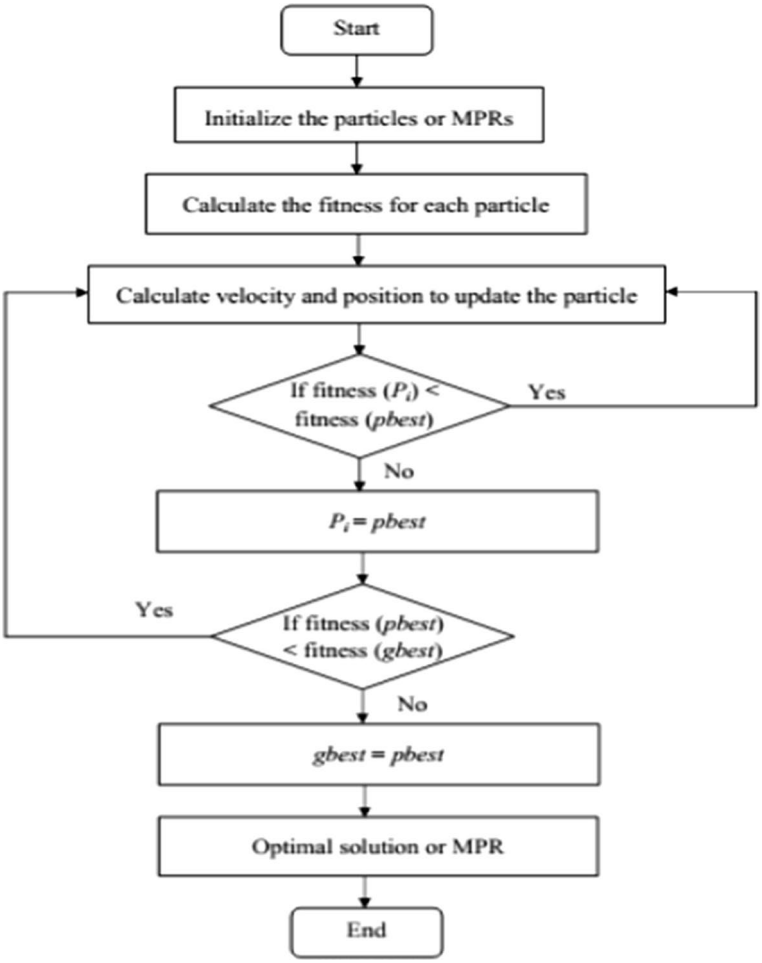

Fig. 4 Flow diagram of the optimal MPR selection

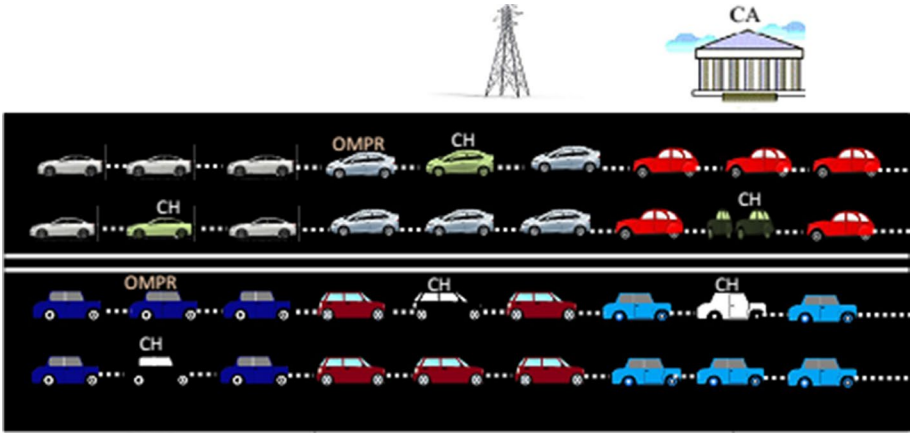

Fig. 5 Optimal MPRs selection

Algorithm

1. Initialize the particles or MPRs.
2. Calculates the fitness for each particle using equation (12).
3. Calculate velocity and position for each particle using equations (13) and (14) respectively.
4. **If** fitness (P_i) < fitness (*pbest*)
   Update the *pbest* particle
   Else
   $P_i = pbest$
   End
5. **If** fitness (*pbest*) < fitness (*gbest*)
   Update the *gbest* particle
   Else
   $gbest = pbest$
   End
6. Iteration is continued until get the optimal solution or MPR.

By selecting these optimal MPRs, OLSR protocol can establish an efficient route between the CHs and the base station. After the establishment of an efficient route, the data packet of the certificate validated vehicle is forwarded from the CH through this established route. After that with the help of symmetric cryptography application, the secure message transmission will take place.

3.5 Secure Transmission

For secure transmission of data packet from the vehicle V_1 (source) to V_2 (destination) through the CHs, symmetric cryptography approach is presented as proposed in our previous work. The prime aim of symmetric cryptography approach is to provide the secured message transmission. It establishes the communication only, after noticed the authentic certificate information from the cluster head. Also it encrypts and decrypts the certificates to enhance the security of the certificates. Then the message will be forwarded through the selected OMPRs as shown in Fig. 6.Process of secure transmission is discussed below.

- All CHslocated inside the region of CA gain a key (certificate) pair of cluster head that related to the neighbor cluster of certificate authority.
- The proposed OLSR protocol helps to identify the destination. Here the destination vehicle may be in similar cluster or different cluster. When the destination is in different cluster, vehicle V1 must find out the location of the destination vehicle V2 before the connection establishment.
- The symmetrical encryption algorithm is performed based on Advanced Encryption Standard (AES) algorithm.
- During the time of communication, the privacy of the cluster member vehicle's are preserved effectively.
- The communication to the destination is classified into two cases, first one is the communication between the vehicles located in a same cluster and the second one is the communication between the vehicles located in different cluster.
- Communication between the vehicles located in a same cluster: Thevehicle V1 must encode the message to be transmitted to destination vehicle V2 by using the key 'k_s'. More over the destination vehicle V2, must able to calculate the key 'k_s' to decrypt the received message. Here the prime factor is, the cluster head must able to receive the key 'k_s' and decrypts the communication of all the cluster member vehicles. Since the CH is elected from the trusted vehicle and it's operation is frequently monitored by the other verifier nodes, the privacy of the message transmission is preserved.

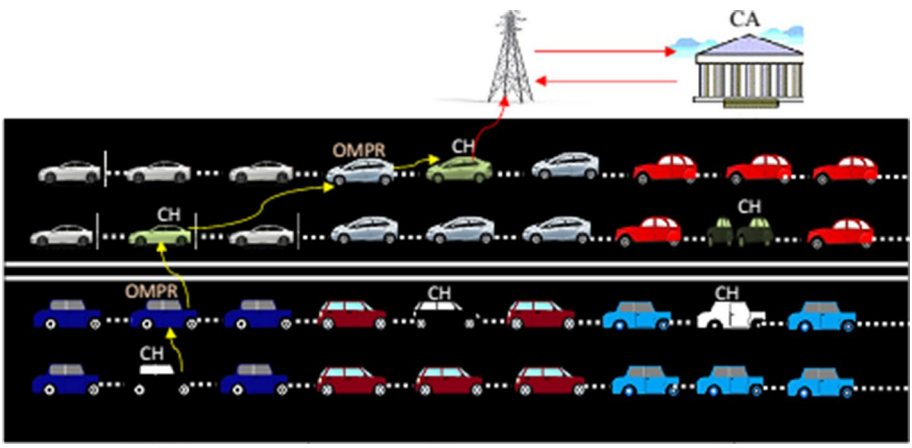

Fig. 6 Secure transmission by selecting the OMPRs

- Communication between the vehicles located in different cluster: When the source vehicle V1 is in need to communicate with the destination vehicle V2 located in different cluster, the cluster head must verify both source and destination and receive the necessary keys by using the corresponding cluster head. After that vehicle V1 and V2 can communicate with each other. If the vehicle node V1 wants to connects with the cluster, it uses its current key to communicate with the vehicle node V2

4 Experiment Results

Our proposed approach OLSR-PSO (OLSR routing protocol using Particle Swarm Optimization with Certificate Revocation Scheme) is implemented in network simulatorNS2.

In this simulation process, five hundred vehicle nodes are placed in 2500 m × 1000 m region. 0.66 W is assigned as transmission power and 0.395 W is assigned as receiving power to all the vehicles in the simulation area. Optimized link state routing algorithm is used in this simulation process. Each vehicle node possesses omni directional antenna and the transmission power is uniform in all the sides. Transmission range of every vehicle node is 250 m. To predict the power of the every received packet, two ray ground radio propagation frame work is used. Table 1 reveals the various parameters used for the simulation and its value.

4.1 Performance Metrics

Performance of our proposed approach is evaluated using the following metrics. Performance metrics of our proposed approach OLSR-PSOare compared with that of LAPR [12] and OLSR [13].

4.1.1 Delivery Ratio

Delivery ratio indicates number of successful arrival of the packet. It is calculated from the following equation.

Table 1 Simulation parameters and its values

Parameter	Value
Area size	2500 m × 1000 m
Protocol used for routing	OLSR
Medium access control	802_11
Type of antenna	Omni antenna
Radio propagation model	Two ray ground
Size of the Packet	512 bytes
Initial transmitting power	0.660 W
Initial receiving power	0.395 W
Initial energy	10.3 J
Simulation time	50 s
Rate	500 kb

$$Delivery\ ratio = \frac{Number\ of\ packets\ received}{Number\ of\ packets\ transmitted} \tag{15}$$

4.1.2 Packet Drop

Packet drop means, total number of packets are dropped or discarded during the transmission. This is occurred because of the unreachable destination, duplicate packet, destination address mismatch etc.,

4.1.3 Packet Delay

Packet delay indicateshow much time takes by the packet to reach the destination. Unit of this parameter is seconds (s).

4.1.4 Throughput

The amount of data packet can be transmitted from the sources node to the destination node within a second is called as throughput. Unit of this parameter is kb/s.

$$Throughput = \frac{Amount\ of\ transmitted\ data\ (kb)}{Transmitted\ time\ (s)} \tag{16}$$

4.1.5 Overhead

Overhead indicates number of additional fields is embedded into the data packet for the transmission of the data packet.

4.1.6 Energy Consumption

During the time of packet transmission, the amount of energy consumed by every vehicle nodes is called as energy consumption. It is the difference between the initial energy and current energy of a vehicle node. Unit of energy consumption is Joule (J).

$$Energy\ consumption = Initial\ energy - current\ energy \tag{17}$$

4.2 Performance Based on Rates

The performance of the proposed OLSR-PSO model is analyzed with the existing algorithm LAPR and OLSR by varying the rates 100, 200, 300, 400 and 500 kb. The comparison of the performance analysis is diagrammatically shown in the Figs. 7, 8, 9, 10, 11 and 12. Figure 7 reveals the analysis of delivery ratio of the OLSR-PSO model with the existing algorithms for varying rates. By presenting efficient cluster head selection using weight based on trust degree, the cluster members are controlled by forwarding the data packet to the destination without the direction of CH the delivery ratio of OLSR-PSO is raised to 31% and 45% than that of existing LAPR and OLSR.

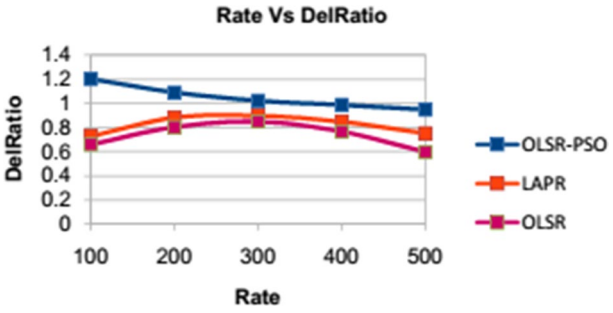

Fig. 7 Rate Vs delivery ratio

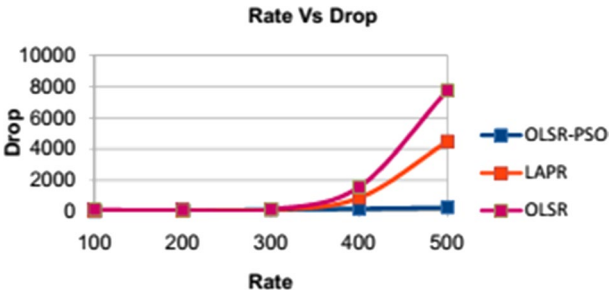

Fig. 8 Rate Vs drop

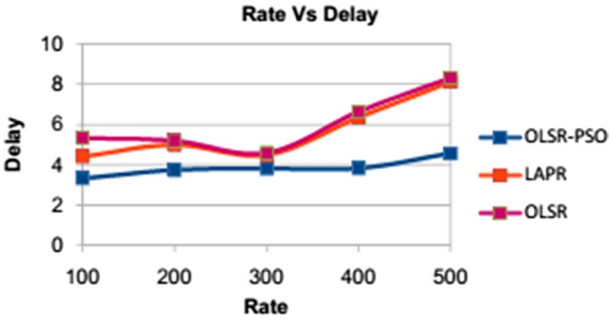

Fig. 9 Rate Vs delay

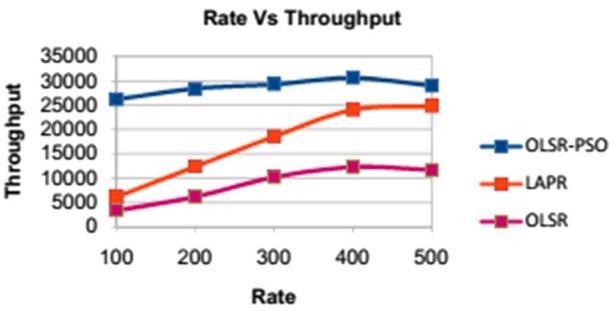

Fig. 10 Rate Vs throughput

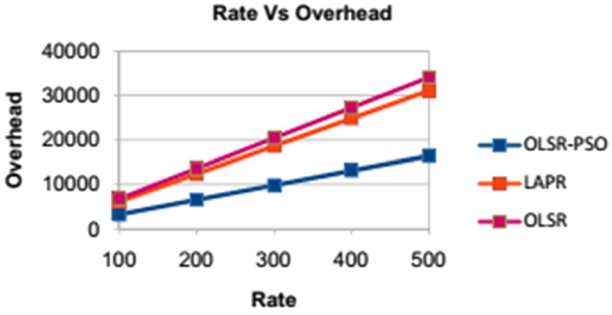

Fig. 11 Rate Vs overhead

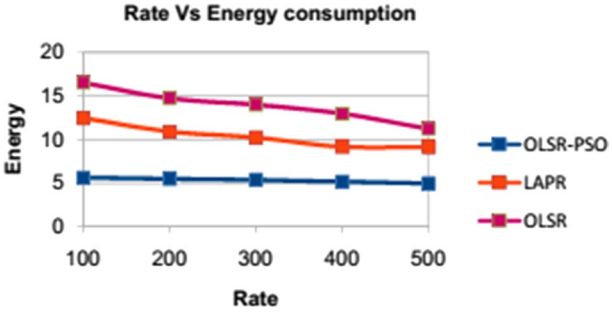

Fig. 12 Rate Vs energy consumption

Figure 8 reveals the comparison of packet drop of OLSR-PSO with the existing work for varying rates. Since the apt route is selected efficiently in OLSR-PSO routing protocol, the number of successful received packets are increased and at the same time the amount of lost packets are declined. From the Fig. 8, it concluded that, compared with the existing LAPR and OLSR, packet drop of OLSR with PSO approach is declined to 4% and 9% respectively. The Fig. 9 represents the comparison of end to end delay of the existing LAPR and OLSR approach with the proposed work varying with rates. Since OLSR-PSO approach, selected the apt node as a CH and immediately revoked the certificates of malicious nodes, the forwarded data packets were reached the destination within the stipulated time. Hence the packet delay of OLSR-PSO protocol is declined to 24% and 28%, when compared with the existing LAPR and OLSR protocols.

Figure 10 reveals the throughput comparison of OLSR-PSO with the LAPR and OLSR work for varying rates. Because of the successful selection of optimal route, the number of data packets transmitted per second is improved and the throughput also increased. When compared with the existing approach, the throughput of the OLSR-PSO protocol is raised to 56% and 84% respectively. Figure 11 shows the overhead comparison of the existing LAPR and OLSR protocols with the proposed OLSR-PSO protocol. Overhead of the proposed OLSR-PSO is declined to 47% and 52% than that of LAPR and OLSR. Figure 12 shows the comparison of energy consumption of OLSR-PSO with the existing work. For the apt selection of cluster head and the successful route selection, the energy consumption is reduced to 48% and 63% respectively, when compared with the existing works.

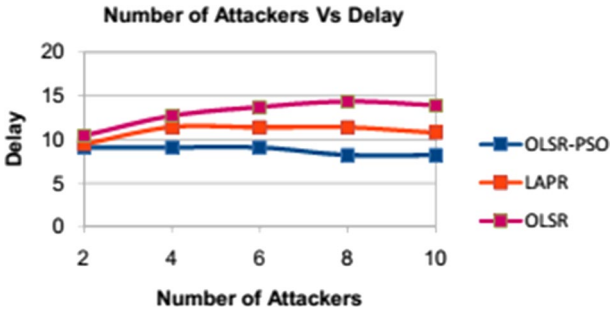

Fig. 13 Number of attackers Vs delay

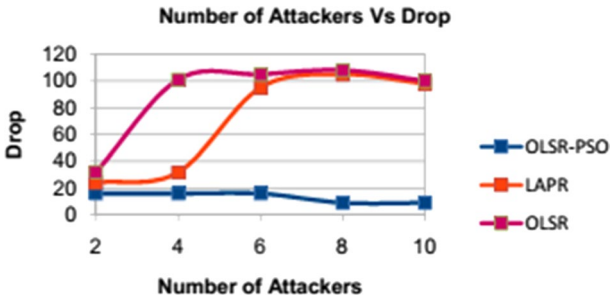

Fig. 14 Number of attackers Vs drop

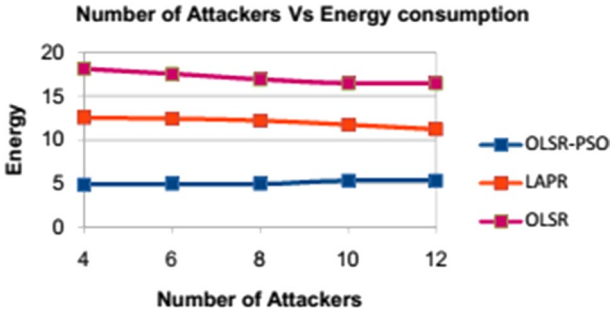

Fig. 15 Number of attackers Vs energy consumption

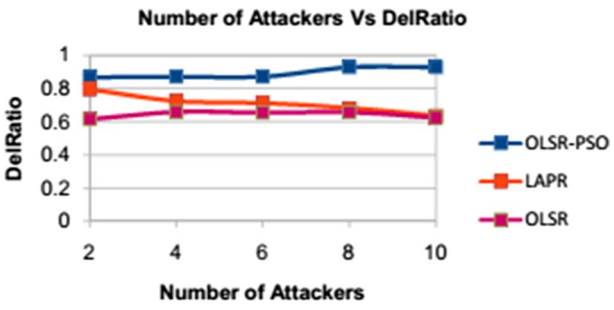

Fig. 16 Number of attackers Vs delivery ratio

4.3 Performance Based on Attackers

The proposed approach OLSR-PSO's performance metrics are evaluated by changing the number of attacker nodes 2, 4, 6, 8, and 10. Figures 13, 14, 15 and 16 demonstrate the performance analysis of OLSR-PSO with the existing work LAPR and OLSR. Figure 13 demonstrates the comparison of end-to-end delay of the OLSR-PSO protocol with the previous work by varying the number of attacker nodes. When compared with the existing works LAPR and OLSR, the proposed OLSR-PSO protocol reduced the delay to 20% and 34% respectively. A comparison of drop and energy consumption of the OLSR-PSO approach with the existing work is ssshown in Figs. 14 and 15 respectively. Packet delay of the OLSR-PSO is declined to 83% and 85% than that of LAPR and OLSR respectively. When compared with the previous approach LAPR and OLSR, the proposed approach energy consumption is declined to 60% and 71%. Figure 16 reveals the delivery ratio comparison of OLSR-PSO with the existing LAPR and OLSR for a varying number of attackers. The delivery ratio of the proposed work OLSR-PSO is increased to 23% and 34% than that of LAPR and OLSR respectively.

5 Conclusion

In this paper, energy-efficient enhanced OLSR routing protocol using Particle Swarm Optimization with Certificate Revocation Scheme for VANET has been presented. The performance of the OLSR-PSO protocol has been evaluated by using the simulator NS2. In this approach, vehicles or nodes in the zone were grouped as a number of clusters by selecting the cluster head using the weight based on trust degree. This trust degree has been calculated using direct and indirect trust degree values. The node with maximum weight has been selected as a cluster head. Node with less trust value than the threshold value was identified and revoked as attacked nodes using the Certificate Revocation List. Then certificates to those attacked nodes were revoked by a certificate authority. Validation of each node in a cluster has been verified by CA before individual transmission. Then the transmission has been done on the apt path and it has been established by using the OLSR-PSO routing protocol. From the simulation results, it is concluded that the energy efficiency of the network has been improved by using the proposed OLSR-PSO routing approach.

Funding There is no funding from any Research or Funding Agency.

Declarations

Conflict of interest The authors declare that we have no conflict of interest.

Data Availability Statement The already existing algorithms data used to support the findings of this study have not been made available.

References

1. Chirayil, G. S., & Ashly, T. (2016). A study on cost effectiveness and security of VANET technologies for future enhancement. *Procedia Technology, 25*, 356–363.
2. Cunha, F., et al. (2016). Data communication invanets: Protocols, applications and challenges. *Ad Hoc Networks, 44*, 90–103.
3. Ali, G. G. M. N., et al. (2016). Efficient data dissemination in cooperative multi-RSU vehicular ad hoc networks (Vanets). *Journal of Systems and Software, 117*, 508–527.
4. Ali, G. G. M. N., Chan, E., & Li, W. (2013). Supporting real-time multiple data items query in multi-RSU vehicular ad hoc networks (Vanets). *Journal of Systems and Software, 86*, 2127–2142.
5. Wu, T.-Y., et al. (2012). Improving RSU service time by distributed sorting mechanism. *Ad Hoc Networks, 10*, 212–221.
6. Sakiz, F., & Sen, S. (2017). A survey of attacks and detection mechanisms on intelligent transportation systems: Vanets and Iov. *Ad Hoc Networks, 61*, 33–50.
7. Tyagi, P., & Dembla, D. (2017). Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET). *Egyptian Informatics Journal, 18*, 133–139.
8. García-Campos, J. M., et al. (2016). An evaluation methodology for reliable simulation based studies of routing protocols in vanets. *Simulation Modelling Practice and Theory, 66*, 139–165.
9. Purohit, K., Dimri, S., & Jasola, S. (2016). Performance evaluation of various MANET routing protocols for adaptability in VANET environment. *International Journal of System Assurance Engineering and Management, 8*, 690–702.
10. Husain, A., & Sharma, S. (2016). Implementation of geographical location based routing protocols in vehicular environment. *International Journal of System Assurance Engineering and Management, 9*, 18–25.
11. Raw, R., Lobiyal, D., Das, S., & Kumar, S. (2015). Analytical evaluation of directional-location aided routing protocol for VANETs. *Wireless Personal Communications, 82*(3), 1877–1891.
12. Husain, A., & Sharma, S. C. (2016). Implementation of geographical location based routing protocols in vehicular environment. *International Journal of System Assurance Engineering and Management, 9*(1), 18–25.
13. Toutouh, J., Nesmachnow, S., & Alba, E. (2012). Fast energy-aware OLSR routing in vanets by means of a parallel evolutionary algorithm. *Cluster Computing, 16*, 435–450.
14. Ganan, C., et al. (2015). EPA: An efficient and privacy-aware revocation mechanism for vehicular ad hoc networks. *Pervasive and Mobile Computing, 21*, 75–91.
15. Daeinabi, A., & Rahbar, A. G. (2014). An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks. *Computers and Electrical Engineering, 40*(2), 517–529.
16. Saleh, A. I., Gamel, S. A., & Abo-Al-Ez, K. M. (2016). A reliable routing protocol for vehicular ad hoc networks. *Computers and Electrical Engineering, 64*, 473–495.
17. Bitam, S., Mellouk, A., & Zeadally, S. (2013). Hybr: A hybrid bio-inspired bee swarm routing protocol for safety applications in vehicular ad hoc networks (Vanets). *Journal of Systems Architecture, 59*, 953–967.
18. Mirjazaee, N., & Moghim, N. (2015). An opportunistic routing based on symmetrical traffic distribution in vehicular networks. *Computers and Electrical Engineering, 47*, 1–12.
19. Liu, H., Yang, L., & Zhang, Y. (2015). Improved AODV routing protocol based on restricted broadcasting by communication zones in large-scale VANET. *Arabian Journal for Science and Engineering*, *40*(3), 857–872.

C. BrijilalRuban received B.E. degree in Electronics and communication engineering from Anna University Chennai. He obtained hir M.E. degree in Computer Science and Engineering under Anna University. He has completed his Ph.D. in Anna University.The area of research is Security in VANETs. Currently He is working as an Assistant Professor in Department of Computer Science and Engineering, in Maria College of Engineering and Technology, Attoor, Tamilnadu, India.

B. Paramasivan received M.E. degree in Computer Science and Engineering under Jadavpur University, Kolkatta, India. He obtained his Ph.D. degree in Anna University, the area of research is Quality of Service in Wireless Sensor Networks. He is working as a Professor and Head in Department of Computer Science and Engineering, National Engineering College, Kovilpatti, Tamilnadu, India. He has published twenty four papers in International and National Journals. He has also presented more than fifteen papers in various International Conferences. He has organized eighteen seminars sponsored by various Governmental agencies. He is the reviewer of five international journal.He is an active member of various professional bodies like IE, CSI, ISTE and IEEE.