Multi-Agent System for Secured and Reliable Routing in VANET

Anil D. Devangavi[1] and Dr. Rajendra Gupta[2]

[1]*Basaveshwar Engineering College, Bagalkot, Karnataka, India*
[2]*AISECT University, Madhya Pradesh, India*

Abstract:- **In VANET, the emphasis is given on the exchange of traffic information and road conditions between the vehicles and thereby preventing the accidents. Distinctive characteristics of VANET like restricted topology, unpredictable mobility, vehicle density, varying channel capacity, etc. make VANET environment exciting for developing efficient routing protocols. Owing to the dynamic topology in VANET, the routes are unstable and unreliable for exchange of information among the vehicles. To enrich the performance and throughput of the VANETs, the links between nodes must be reliable and stable. In order to tackle the relaiblity and stability of information communication this work proposes 'Multi-agent system for Secured and Reliable Routing (MSRR) in VANET. The performance of the proposed scheme is tested in terms of packet delivery ratio, route reliability, route discovery time and delay.**

Keywords- **VANET, Multi-agents, Trust value, Reliability weight, Route Discovery Time and Delay.**

I. INTRODUCTION

Vehicular Ad hoc Network (VANET) is a class of Mobile Ad Hoc Network (MANET) and one of the core technologies in Intelligent Transportation Systems (ITS)[25]. VANET's have an edge over MANETs in having sufficient computational and power resources equipped with each vehicle. This eliminates energy related computations in VANETs.

VANET comprises of a group of moving vehicles and some fixed infrastructure. The primary architectures for vehicular communication in VANETs are Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) and Hybrid Architecture [16]. Recently, Vehicle-to-Passenger communication (V2P) is being discussed, which can be possible by fourth architecture. V2V communication is primary constituent of ITS. It enables the vehicle to communicate with other vehicles. V2I is the communication between vehicles and roadside infrastructure, intended primarily to enable a wide range of safety, mobility and environmental benefits. Hybrid architecture integrates both V2V and V2I communication architectures. Vehicle-to-Passenger communication allows straight, immediate, and adjustable communication between moving vehicles and roadside passengers.

The routing protocols of VANET are broadly classified as: topology based routing protocols, position based routing protocols, cluster based routing protocols, broadcast routing protocols and geo cast routing protocols and [6][34]. The topology based routing protocols makes use of existing links information in the network to forward the packets. Position based routing protocols use geographic positioning information in order to select the next forwarding. In cluster based routing protocols, the entire network is divided into clusters. Thus an interconnected set of clusters are identified. Broadcast routing protocols are used when message needs to be sent far distant vehicle by using multi-hop communication. Geo cast routing protocols are a variety of location based multicast routing and used in VANET to deliver the packet to all nodes within a stated geographical area.

Distinctive characteristics of VANET are restricted topology, unpredictable mobility and vehicle density, varying channel capacity etc. [20]. Because of the dynamic topology, routes are frequently broken and are unreliable. Thus in VANETs, the task of developing reliable routing protocols is very challenging.

1.1 Related Work

A novel infrastructure based connectivity aware routing protocol iCAR-II which enables multi-hop vehicular applications is presented in [1]. iCAR-II consists of algorithms that are run by vehicles to calculate local networks connectivity. The real time information is used to continuously update location servers. A global network topology is thus generated. Authors in [2] have presented a token based trust computation technique, which relies on network connectivity duration of vehicles in VANET. The presented technique is based on travelling time association among vehicles or network connectivity of vehicle at the time of driving on the road.

Authors in [3] have reviewed the most recent Traffic Aware Routing (TAR) protocols while stressing on traffic and network conditions awareness issues. Also authors have explored the strengths and weaknesses of TAR protocols with respect to measurement of routing metrics, forwarding mechanisms and recovery techniques.

A Reliable Routing Protocol (R2P) for VANETs divides the network into overlapping zones, which is given in [8]. Amongst the nodes in each zone, one node is designated as a Master Node (MN). Master node maintains up-to-date routing boards for inter/intra-zone communication. R2P employs a special route discovery mechanism to discover available

routes to the destination and then elects the most reliable route. Improved distance-based VANET routing protocol in urban traffic environments is presented in [9]. The distance based protocol is applied to multi-hop broadcast scheme for reliable packet dissemination, which is based on stable routing decisions schemes.

A Multi level-scenario-oriented Greedy Opportunity Routing protocol (M-GOR) is depicted in [10]. A calculation method for the connectivity probability and a Greedy Opportunity Forwarding (GOF) algorithm to respond to the impacts of the multilevel structure is presented.

An extension of reliable Ad-hoc On-demand Distance Vector routing protocol (AODV), AODV-L is given in [13]. The authors have used vehicles movement information to predict the stability period of a route. Moving vehicles transmission range is computed based on state of the channel. A position-based routing approach for VANET is presented in [14]. Authors have considered the obstacles (building, tree, etc.) blocking radio transmissions and voids, present in a city environment.

The use of modified AOMDV protocol is given in [15]. AOMDV and AODV are compared in terms of different traffic pattern of UDP and CBR. In the multipath routing protocol an alternate path from source to destination is selected when ongoing path is failed.

An intelligent multihop routing protocol that interacts with the environment and learn the best transmission parameters is presented in [17]. The protocol use the parameters like data transmission rate, vehicle movement, and route length. Authors in [19] present Long Lifetime Any paths (LLA) routing scheme that has utilized the metric of link cost based on the introduced link stability index. The authors focus on anypath routing to improve the reliability of multihop VANET communications. Authors in [20] present an improved DSDV routing protocol MA-DSDV based on multi-agent system approach. In this approach, each agent periodically broadcast its routing table with a sequence number to keep track of the recently broadcasted information.

Multi agent based system for congestion control is illustrated in [21]. In the presented scheme, the agents in the nodes listen to the status of neighbouring node information. Based on neighbour node information, congestion free path is computed. A new routing protocol Multimetric Map aware routing protocol (MMMR) for VANETs that uses several metrics like distance, direction of vehicles, number of vehicles and bandwidth to calculate the multi metric value for the next forwarding nodes is given in [22]. The node with better value is decided as the next node.

Authors in [24] present a Secure and Intelligent Routing (SIR) protocol to find quick and secured path. The scheme calculates trusted vehicles at every junction, which acquires the information of the neighbouring vehicles and compute the secured path. Authors in [26] describe the usage of extended evolving graph theory to develop a link reliability model based on the speed and movements of the vehicles on a highway. Velocity of the vehicles is used to calculate link reliability. Reliable routes are computed pre-emptively.

The authors in [27] present an event triggered multipath routing in WSNs by employing a set of static and mobile agents. In this scheme, the node generating the event knows about location information of destination node and computes arbitrary midpoint between itself and the destination node. A new vehicular reliability protocol AODV-R to calculate reliable routes in VANETs is presented in [28]. The link reliability is defined as the probability that a communication link between two vehicles will not break for a specified time period and is accurately calculated using the information of vehicles along the road.

A class of routing protocols called Road-Based using Vehicular Traffic information routing (RBVT), a reactive protocol RBVT-R and a proactive protocol, RBVT-P are presented in [33]. The protocols create paths consisting of road intersections having connectivity of high probability. The authors in [35] described the usage of vehicles movement information to predict the chance of a link-breakage event. Vehicles are grouped based on their velocity. A scheme that secures geographic position-based routing is presented in [36]. The scheme safeguards the position-based routing services likerelay communication, accurate location service and etc. thereby increasing the robustness of the network.

Some of the drawbacks of existing routing techniques ACO-based MCQ aware (S-AMCQ) [4], Stable Routing Protocol (SRP) [7], Organized Topology Based Routing (OTBR) [11], Greedy Bundle Release Scheme-Bulk Bundle Release (GBRS-BBR) [30] and Vehicle Heading Based Routing (VHBR) [38] in addition to the ones mentioned in related work are as follows: (i) Lack of intelligence in path discovery and path construction, (ii) lesser flexibility in relay node selection mechanisms, (iii) lack of robust mechanism for critical information transmission and (iv) reliability of constructed routes is less and etc.

In VANET, vehicles exchange the traffic and other warning information with each other during travelling. In these networks, high mobility of the nodes is the major concern, due to which routes are frequently broken. Hence the dynamics of vehicle topology makes the routes unstable and unreliable for exchange of information among the vehicles. To tackle these issues, we have proposed *Multi-agent System for Secured and Reliable routing* (MSRR) in VANET. The proposed work facilitates computation of reliable and secured that enhances the performance of the proposed system.

1.2 Methodology

The proposed MSRR protocol calculates secured and reliable path between the source and destination using agent technology. For faciliatating the reliable and stable communication, the proposed protocol uses the agent

technology. For compuatation of the route the proposed protocol uses two different agencies viz *Vehicle Agency* (VA) at each vehicle and *Road Side Unit* Agency (RSUA).

The proposed scheme works as follows: (1) Static agent in the source vehicle calculates ***'n'*** favourable vehicle nodes (vehicle nodes in the direction of destination based on neighbourhood information). (2) Static agent in the source vehicle node triggers a mobile agent and creates ***'n'*** clones of it. (3) Each clone of mobile agent traverse through one favourable node (one to one mapping of '***n'*** clones to '***n'*** favourable nodes) towards destination node calculating the next intermediate nodes based on neighbourhood information. (4) Whenever any two clones meet at any intermediate vehicle node, a static agent is triggered at that intermediate node to evaluate the best path amongst the paths traversed by the two clones. (5) Clone with the best path is allowed to traverse further and the other clone is terminated. (6) This process continues until best path to the destination is computed. (7) Information is encrypted and transmitted along the path. (8) During the transit of the information, if any of the next intermediate node is malicious (has moved out of the network and etc.), then from the current vehicle node another intermediate vehicle node is computed and a patch up path is calculated.

Some of the contributions of the proposed routing technique are as follows: (1) Usage of static node for the computation of favourable nodes. (2) Usage of mobile agent clones for traversing through the favourable nodes computed. (3) Defining and usage of trust value for the selection of intermediate nodes. (4) Defining and usage of reliability weight factor to calculate the best reliable path. (5) The performance of the proposed scheme is tested in terms of performance parameters such as packet delivery ratio, route reliability, route discovery time and delay.

The proposed work is compared with AODV-L [13]. The advantages of proposed MSRR over AODV-L are as follows: (1) Use of multiple agents for finding the path from source to destination node. (2) Reliable delivery of the critical information. (3) As it uses the trust value to select every relay node, the selected path is more secured. (4) Path construction mechanism is incremental and has progressive accuracy and (5) best path is computed based on reliability weight factor.

II. STRUCTURING THE PROPOSED SYSTEM

This section presents the network environment, mathematical models, proposed agency, scheme and algorithm.

2.1 Network Environment

Figure 1 presents the network environment in which we can notice that number of vechiles move with different speed in different lanes. Some of the assumptions in this work are: vehicles travel in an urban road scenario, each vehicle is fitted with Global Positioning System (GPS), sensors and on-board communication devices for communication. The information regarding location and direction of the vehicle is provided by GPS. Each vehicle is fitted with a digital map, which provides information regarding road connectivity. It is also assumed that on-board communication devices are inbuilt with an agent platform and the platform supports our proposed agency [20] [21] [31]. Agency involves static agents, mobile agents and a knowledge base. Agents are guarded from hosts on which they execute and vice versa. The platform is completely secured.

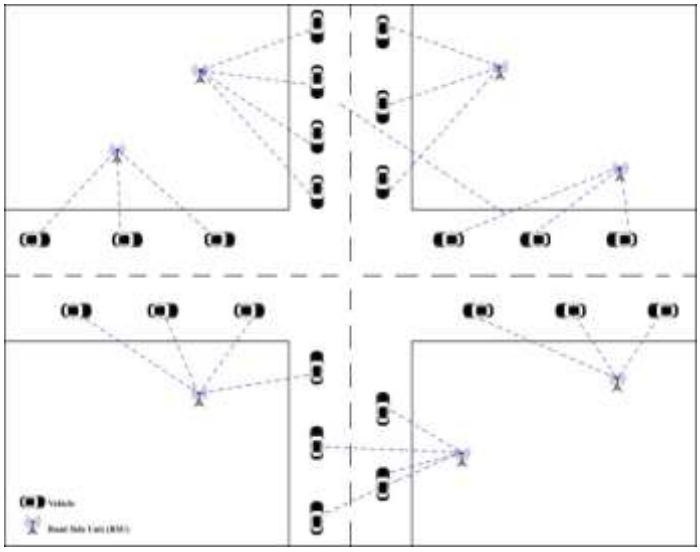

Figure 1. VANET Environment-Urban Scenario

Each vehicle communicates with other vehicle within its communication range (V_{Ran}) via V-to-V communication. The vehicles that lies within the transmission range of a particular vehicle are the neighbouring vehicles of that vehicle. Each vehicle status is being updated by itself and neighbouring vehicles in a local database. The information is related to vehicle ID, position of the vehicle in terms of latitude and longitude, current speed of the vehicle, direction, trust value and etc. Every vehicle is connected to at least one road side unit (fixed infrastructure). Each vehicle communicates with road side units via V-to-R communication.

Terminology

- *Neighbour vehicles/nodes*: Vehicle nodes which lie in the transmission range (VRan) of vehicle 'V'.
- *Favourable vehicle node (V_{FN}):* It is the vehicle node with trust value C or P (if there are no vehicles with C value), same speed and are in the direction of the destination vehicle node. For any vehicle there may be several favourable vehicle nodes towards destination vehicle. Vehicles with trust value N are ignored.
- *Intermediate vehicle node (V_{IN}):* It is the vehicle node with trust value as C or P (if there are no vehicles with C value), same speed and direction as the destination node. It is the most favourable vehicle node from current vehicle node. Vehicles with trust value N are ignored.

- *Best Path / Reliable Path:* Best path is the path with higher reliability weight factor.

2.2 Mathematical models

In this subsection, mathematical models for reliability weight and trust value are derived.

2.2.1 *Mathematical Model for reliability weight*

Reliability weight of any path between two vehicle nodes is computed as follows. Let

M_{AV}: Average mobility/speed of the vehicles on the path and is measured in Kmts./hr.

N_{IP}: No. of Intermediate nodes (V_{IN}) in the path.

N_{PN}: No. of intermediate nodes in the path with partial trust value 'P'.

D: Distance between the two end vehicle nodes of the path and is measured in mts.

For any 2 nodes (X1, Y1) and (X2, Y2), D= $\sqrt{(X_2-X_1)^2+(Y_2-Y_1)^2}$

N_T: Numerical representation of trust value of the end vehicle node.

Reliability weight of any path (W_{RT}) is directly proportional to the number of intermediate nodes N_{IP} and numerical representation of the trust value N_T and is indirectly proportional to average mobility of the vehicles in the path M_{AV}, number of intermediate vehicles with P as trust value N_{PN} and the distance between the source vehicle and destination vehicle D (Eq. 1).

$W_{RT} \alpha N_{IP}$

$\alpha 1/ M_{AV}$

$\alpha 1/ N_{PN}$

αN_T

$\alpha 1 / D$ ..... (1)

i.e. $W_{RT} \alpha N_{IP} * N_T / M_{AV} * N_{UN} * D$ .....(2)

From the Eq. 1 and Eq. 2 reliability weight of any path from the source to the destination with n nodes in the path is computed as:

$$W_{RT} = \sum_{i=0}^{i=n} \left(N_{IP} * N_T * / M_{AV} * N_{PN} * D \right) \quad \text{.....(3)}$$

2.2.2 Mathematical Modelling of Numerical representation of trust value:

Every vehicle is connected to atleast one RSU at any given time. RSU allocates trust value to each vehicle. Trust values are of three types: *Completely trusted* (C), *Partially trusted* (P) and *Not trusted* (N). Trust value is subjective and time dependent. Initially every vehicle is assigned with trust value of '*C*'. Then afterwards the trust value is either retained as '*C*' or changed to '*P*' or '*N*' based on constraints like *time aging factor* and *positive or negative interactions*.When the intermediate vehicle not only transmits a packet to all its next hops, but also forward devotedly (correct modification if essential), then it is positive interaction. But in case of negative interaction the intermediate vehicle does not forward packet correctly by launching some attacks like black hole attacks and etc.

- ***Time aging factor*** *(T_F) :* It indicates that the trust fades with time (lesser faith on vehicles with longer duration on road) during the time period Δt w.r.t. the current time.
- ***Positive interactions*** *(P_I)* : No. of Interactions of the vehicle forwarding a packet to all its next hops devotedly (correct modification if essential) during the time period Δt w.r.t. the current time.
- ***Negative interactions*** *(N_I)* : No. of Interactions of the vehicle that does not forward the data by launching some attacks like black hole attacks and etc. during the time period Δt w.r.t. the current time [12][23].

Numerically the trust values are represented as: $C \rightarrow 1$, $P \rightarrow ½$, $N \rightarrow (-1)$.

2.3 RSA algorithm

The proposed work uses RSA algorithm for secured data transmission. The reason behind using RSA algorithm is that (i) It is based on Public Key encryption in which the information is encoded with someone's Public Key (everyone knows Public Key). Nevertheless, only the intended person can read it, by using their private key (which only they know about). Endeavouring to utilize the Public Key to decode the message would not work. (ii) The security of the RSA calculation has so far been approved, since no known endeavours to break it have yet been fruitful, generally because of the trouble of factoring n = pq, where p and q are huge prime numbers [18] [29] [42].

2.4 Proposed Agency

Various agencies [5] are employed to perform communication among vehicles and road side units viz. Vehicle Agency, Road Side Unit Agency.

2.4.1 Vehicle Agency

Vehicle agency resides in each vehicle. Vehicle agency works on the principle of black board architecture for inter agent communication and coordination. The components of vehicle agency and their interaction is depicted in Figure 2. Vehicle agency consists of a set of agents viz. *Vehicle Information Manager Agent* (VIMA), *Destination Path Finder Agent* (DPFA) and *Path Evaluator Agent* (PEA). The vehicle agency also consists of a *Vehicle KnowledgeBase* (VKB).

Vehicle Information Manager Agent (VIMA): Vehicle Information Manager Agent (VIMA) is a static agent in each vehicle. VIMA monitors the information like *transmission*

range and *time stamp*. It gets information like *Vehicle/Node ID, location in terms of latitude and longitude, speed of the vehicle, direction of the vehicle and trust value* [2] [12] [23] from the neighbour nodes. It also shares similar information of the parent node with the neighbour nodes. It triggers a mobile agent, *Destination Path Finder Agent (DPFA)* to find the path to the destination vehicle and a static agent, *Path Evaluator Agent (PEA)* to evaluate the best path whenever required. VIMA of the source vehicle node computes a set of favourable vehicle nodes.VIMA of intermediate vehicles computes next neighbour/intermediate node depending upon the neighbour node parameters.

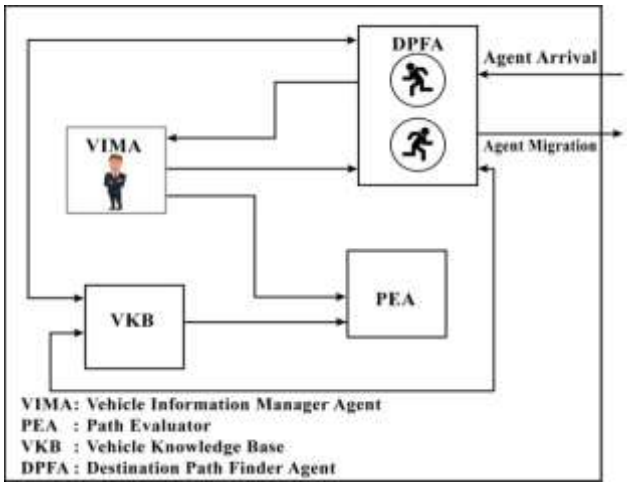

Figure 2. Node/Vehicle Agency

Vehicle Knowledge Base (VKB): It works on the principle of black board architecture. The knowledge base is updated by the agents. It forms the base for inter agent communication and coordination. It maintains *transmission range*, and *time stamp* information of parent node and information like *Node ID, location in terms of latitude and longitude, speed of the vehicle, trust value and direction of the vehicle* of the parent and neighbour vehicles/nodes.

*Destination Path Finder Agent (DPFA)**:* DPFA is a mobile agent and is triggered by VIMA whenever a new path is to be computed to destination vehicle. Multiple clones of DPFA are created. The number of clones is equal to the number of favourable nodes of the source node. Each clone migrates from source vehicle to one favourable node. DPFA clones traverse the network in multiple directions towards destination. Multiple paths are thus explored. While migrating DPFA collects the path information like *distance between the vehicles*, *no. of vehicles* and etc. Finally upon reaching the destination, the path is updated with the parent vehicle node.

Path Evaluator Agent (PEA): Whenever more than one clone meets at any intermediate vehicle node, VIMA of that intermediate vehicle node triggers *Path Evaluator Agent* (PEA).This is a static agent residing in each vehicle and is responsible for finding the best path explored by the different clones. It collects the path information like *distance between the vehicles*, *no. of intermediate vehicles*, *average mobility*, *number of nodes with partial trust values*, *number of untrusted nodes* from each clone. Using this information it computes the *reliability weight* of the paths explored by the different clones. The path with better *reliability weight* is selected as the best path.The same information is communicated to the VIMA of the event node and parent node.

2.4.2 *Roadside Unit Agency:* Roadside Unit Agency resides in each Roadside Unit. It comprises of *Roadside Unit Manager Agent* (RUMA), *Trust Value Allocation Agent* (TVAA) and *Roadside Unit Knowledge Base* (RUKB). The interaction of various components of Roadside Unit Agency is as shown in the Figure 3.

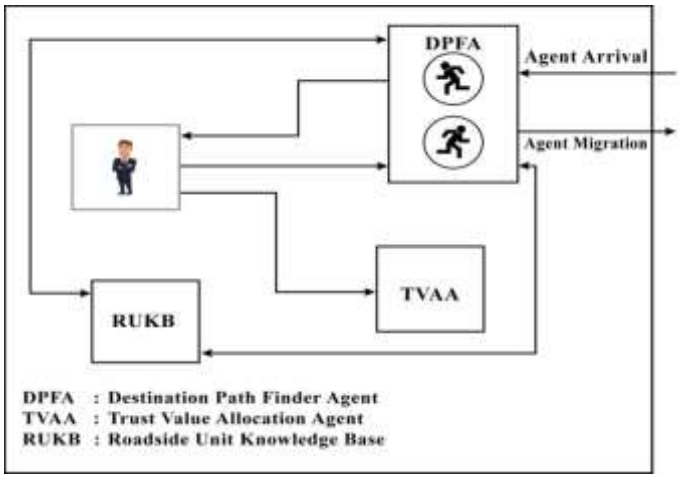

Figure 3. Road side unit Agency

Roadside Unit Manager Agent (RUMA): This is a static agent and resides in the Roadside Unit. Each vehicle is connected to atleast one RSU. It collects information like *Node ID*, its *direction*, *speed* and other information from all the vehicles directly connected to the Roadside Unit. It shares the same information with the neighbour Roadside Units.

Roadside Unit Knowledge Base (RUKB): It works on the principle of black board architecture. The knowledge base is updated by the agents. It forms the base for inter agent communication and coordination. It maintains the information of connected vehicles such as *Node ID*, *location in terms of latitude and longitude*, *speed of the vehicle*, *trust value*, *direction*. This information can be shared with other RSU. It maintains the trust parameters of the vehicles like *time aging*, *positive interactions* and *negative interactions*.

Trust Value Allocation Agent (TVAA): This is a static agent residing in the Roadside Unit. It is responsible for allocating trust value to each connected vehicle. Trust allocation scheme works as follows. All vehicles are connected to at least one RSU and all vehicles involve in the forwarding of the data. Three types of trust value are allocated: *C: Completely trusted*, *P: Partially trusted* and *N: Not trustworthy* [2].

TVAA collects trust parameters like *time aging factor, positive and negative interactions* of each vehicle connected to the parent RSU [12][23]. Trust value is subjective and time dependent. Initially each vehicle will be allocated with trust value *'C'*. If either of the parameters viz. time aging factor and positive interactions is false then the vehicle is assigned the trust value of *'P'* or *'N'* , if both are false. Periodically the trust value of each vehicle is updated by TVAA based on the trust parameters i.e. either continued as

'C' or Updated to *'P'* or *'N'*.

2.5 Example execution of the algorithm to evaluate the best path whenever more than one clone meet at any intermediate node:

Figure 4 illustrates the scenario where three favourable nodes (V_{FN}) for source vehicle **Vs** are computed. Three clones C1, C2 and C3 are triggered and they start exploring through the three computed favourable nodes. Every intermediate vehicle is selected based on neighbourhood parameters and trust value. Two clones C1 and C2 meet at the same intermediate vehicle node V_{IN}. Path 1 and 2 are the two paths traversed by the two clones till V_{IN}.

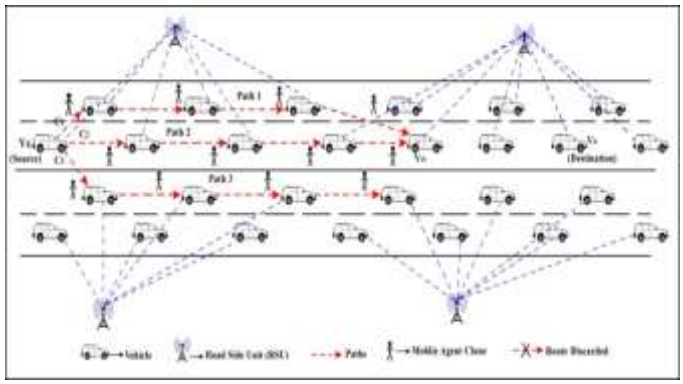

Figure 4. Illustration of two clones meeting at the same vehicle node V_{IN}

Static agent VIMA of V_{IN} triggers path evaluation agent (PEA). PEA computes the reliability weight of both paths 1 and 2 traversed by the two clones. Path 1 has the higher reliability weight and thus it is the best path of the two. Clone 1 is allowed to continue and clone 2 is terminated and the path traversed by it is discarded as shown in the Figure 5.

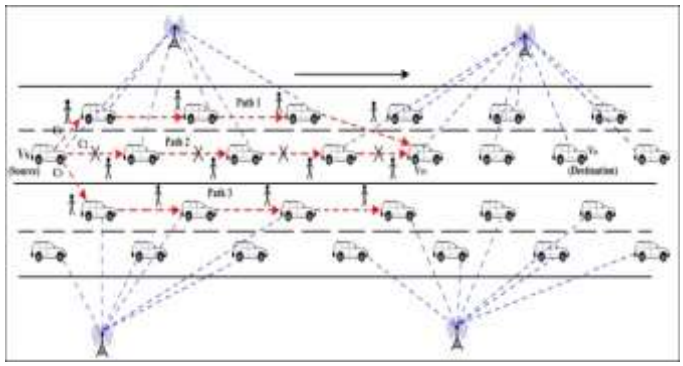

Figure 5. Illustration of retaining the clone traversing the best path

Figure 6 depicts the situation where clone 1 and clone 3 are traversing towards the destination vehicle.

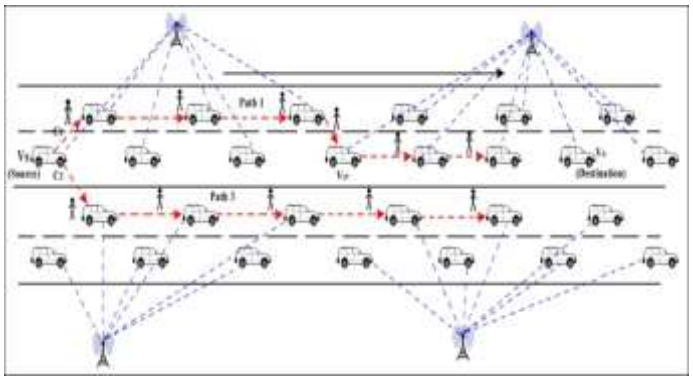

Figure 6. Illustration of retained clone 1 and clone3 moving towards the destination

Figure 7 illustrates two clones C1 and C3 meeting at the destination vehicle. Thus there are two paths from source vehicle Vs to destination vehicle V_D.VIMA of the destination triggers PEA agent to evaluate the best path.

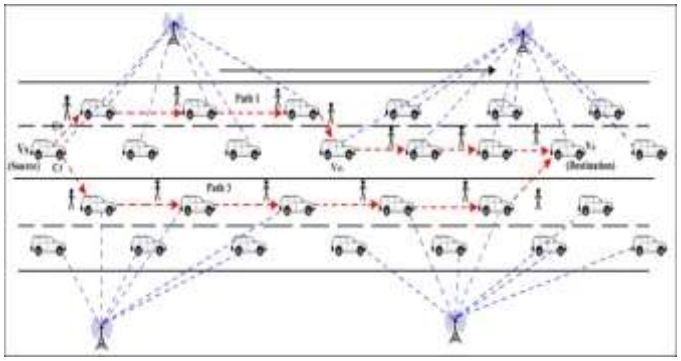

Figure7. Illustration of clone 1 and clone 3 meeting at the destination vehicle

Figure 8 illustrates PEA computing the reliability weight of both the paths 1 and 3. Path 1 has better reliability weight factor and is the best path. Path 3 is discarded.

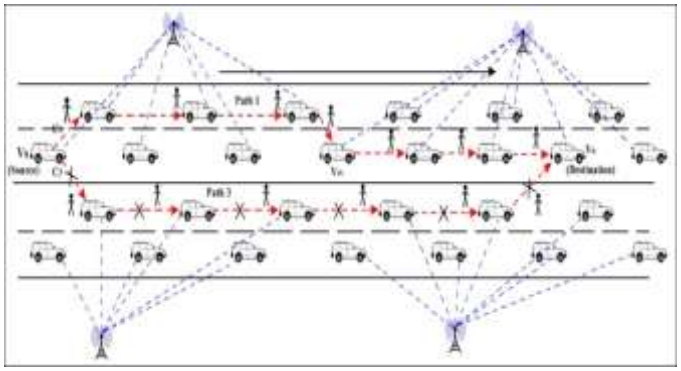

Figure 8. Illustration of elimination of path with lower reliability weight factor

Path 1 is the best path. Information is encrypted by using RSA algorithm and communicated as shown in the Figure 9. As each intermediate vehicle on the path is calculated based on

neighbourhood parameters and trust value, the path is secured. Also as the path is computed based on the reliability weight factor, it is reliable.

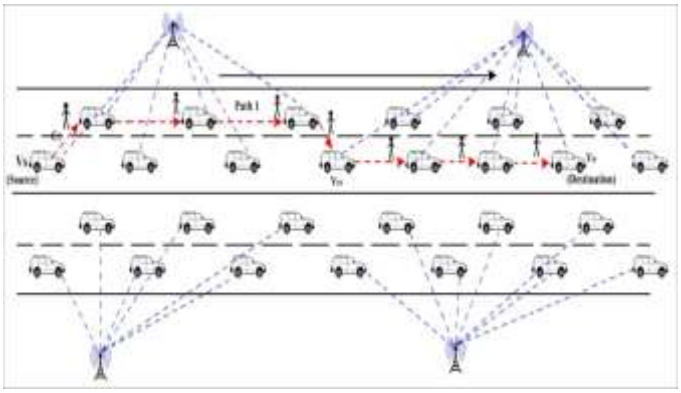

Figure 9. Reliable path from source vehicle to destination vehicle

Example scenario to compute patch up path in case of malicious intermediate node

During the transit of the information the intermediate vehicle node next to current vehicle node V_{IN} is malicious as shown in the figure 10. A patch up path is required.

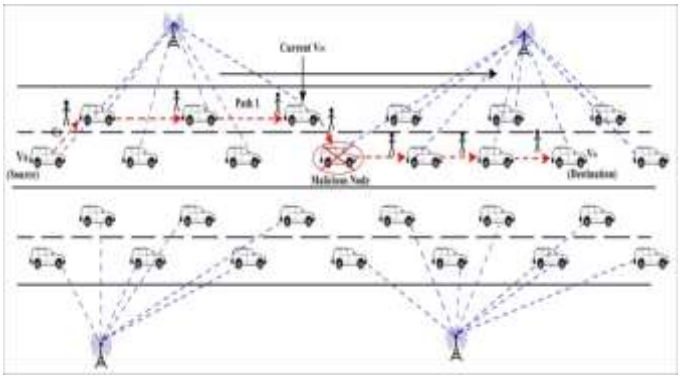

Figure 10. Illustration of one of the malicious intermediate vehicle node

From the current intermediate node V_{IN} another intermediate vehicle node is calculated based on neighbour node information and a patch up path is set to destination as depicted in the Figure 11.

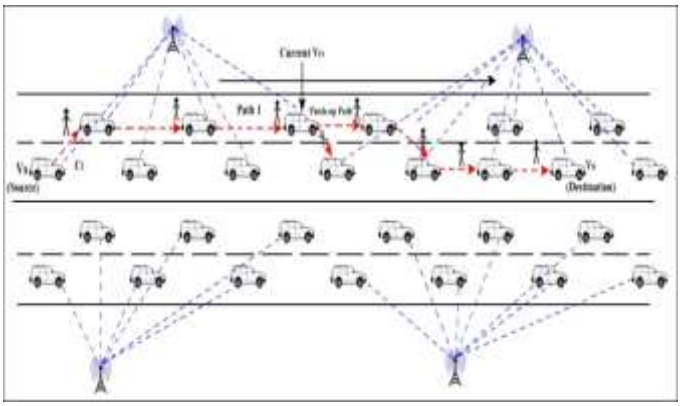

Figure 11. Illustration of computation of patch up path

2.6 Proposed Scheme

This subsection presents the proposed scheme. The steps involved in the proposed scheme are as follows:

(1) Given a source node and destination node.

(2) VIMA of the source node computes *'n'* favourable nodes (V_{FN}). Favourable nodes are the ones with trust value *'C'* or *'P'*, same speed and are in the direction of the destination node. VIMA triggers Destination Path Finder Agent (DPFA) and creates *'n'* clones of DPFA.

(3) Each clone migrates to one favourable node (*'n'* clones and *'n'* favourable nodes with one to one mapping).

(4) VIMA of the favourable nodes (V_{FN}) calculate the next intermediate vehicle node (V_{IN}) amongst its neighbours by considering neighbour node information. The node with trust value as *'C'* or *'P'* (if there are no vehicles with *'C'* value), same speed and in the direction of the destination vehicle node is selected as the next intermediate vehicle node. Node with trust value *'N'* is not considered.

(5) Further next intermediate nodes (V_{IN}) for the nodes determined in step 5 are calculated until the destination node is reached. *'n'* different multiple paths towards destination are thus initiated and explored.

(6) Whenever any two clones meet at any intermediate vehicle node (V_{IN}) in the process of moving towards the destination, VIMA of that vehicle node triggers PEA in that node. PEA calculates reliability weight factor [Eq. 3] of the two alternative paths explored by the two clones till this node [27]. Path with higher reliability factor is considered as the best path and the clone along the best path is allowed to survive and continue towards the destination. The other path is discarded and the clone along that path is terminated by VIMA.

(7) Finally only one clone with the best path survives with the destination node. This clone updates the computed path with the VIMA of source node.

(8) Information is encrypted using RSA algorithm[18] [29] [42].

(9) Encrypted Information is communicated along the best path.

(10) During the transit of the information if any of the next intermediate node (V_{IN}) is malicious (has moved out of the network, and etc.) then from the current vehicle node another intermediate vehicle node is computed and a patch up path is calculated.

2.7 Algorithms

This subsection presents the algorithms for the proposed scheme.

*2.7.1 Algorithm for compting the path between the source vehicle and destination vehicle is as below***:**

Input: A set of vehicles V= {V1…..Vn}.Vs and Vd belongs to V.

A set of RSUs R= {R1……Rn}.

Each vehicle is connected to atleast one RSU and has vehicle agency, RSU has RSU agency.

Output: Reliable and secured Path between the source vehicle and destination vehicle.

Algorithm 1:To compute the reliable path between the source vehicle and destination vehicle

Begin

1. VIMA of Vs calculates 'n' V_{FN} s for Vs;
2. VIMA of Vs triggers mobile agent DPFA and create 'n' clones of it;
3. Each clone traverses through one V_{FN} (one to one mapping);
4. VIMA of each V_{FN} calculates the next V_{IN} for the clone of that particular V_{FN};
5. Each clone of V_{FN} traverses to its next V_{IN};

Do

6. VIMA calculates next V_{IN} for the clone;
7. Each clone traverse to the respective next V_{IN};
8. If any two clones meet at the same V_{IN},
9. VIMA of that V_{IN} triggers PEA to evaluate the best path amongst the paths traversed by the two clones;
10. PEA calculates the best path.
11. Retain clone traversing the best path, terminate the other clone;

Until next V_{IN} is not V_D;

12. Best path is communicated to VIMA of Vs.
13. Information is encrypted using RSA algorithm and communicated. Go to End;
14. If during the transit of information any of the next V_{IN} is malicious (has moved out of the network, and etc.) then from the current vehicle node another intermediate vehicle node is computed and a patch up path is calculated;

End

2.7.2 Algorithm 2: To assign trust value

Algorithm 2:To assign trust value:

Begin

1. For every vehicle $\mathbf{V_i}$ connected to RSU;

If

2. T_F = New and $P_I > k$ where k is a constant and time interval Δt;
3. Trust value= 'C';

Else if T_F= Old and $P_I > k$;

or T_F= New and $P_I < k$;

4. Trust value = 'P';

Else Trust value= 'N';

End

III. SIMULATION MODEL

In this section simulation models, simulation procedure and performance parameters are discussed. We have simulated proposed model by considering Bangalore city map [37] as shown in Figure 12. Only dense traffic roads and urban road scenario are considered for simulation. The simulation is carried out using NS-2.34 [32] to test the performance and effectiveness of approach.

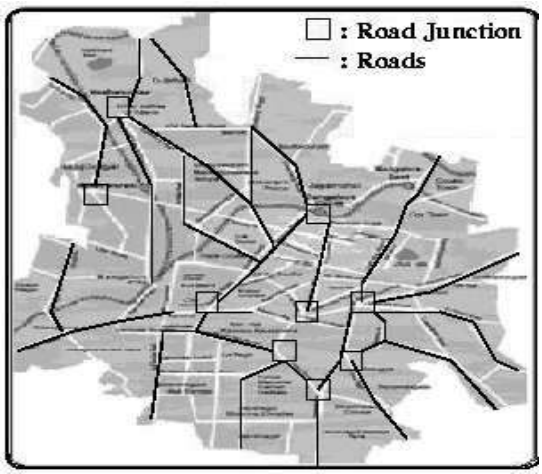

Figure 12. Bangalore City Map [37]

The proposed scheme has been simulated in various VANET scenarios. Simulation environment for the proposed work consist of following models: (1) Network model, (2) Traffic model, (3) Mobility model and (4) Channel model. These models are given below.

Network model: We consider V number of vehicles moving in a fixed region of length X Km. and breadth Y Km. Vehicles are equipped with number of sensors i.e., S1,...Sn. We assume vehicles to move in a freeway type road, with L lanes. Communication coverage area for each vehicle is considered as V_{Ran} meters.

Traffic model: Constant bit rate model is used to transmit certain number of fixed size packets, P pkts. Coverage area around each vehicle has a bandwidth, B_W, shared among its

neighbours. Arrival rate of information (critical/noncritical) into the vehicle follows Poisson distribution with mean λ. Poisson process is used as it is an efficient method for arrival process of events to a queuing system.

Mobility model: At the beginning of a simulation, vehicles are randomly put on the roads. They then move continuously according to history-based speeds. Safety distance of R meters is maintained from preceding vehicle for a certain tolerance time and then change lane if possible. It is assumed that there is a free flow movement of vehicles and the situation of congestions are ignored. It is also assumed that all vehicles are furnished with a communication device and knows start position, start time of vehicle, route that it selects and speed at which it travels.Manhattan mobility model is used for Bangalore city scenario[41]. This mobility model is mainly proposed to simulate the movement in urban area, where the streets are in an organized manner.

Channel model: Communication medium access protocol considered for simulation is Enhanced Distributed Channel Access (EDCA) based Distributed Coordination Function (DCF) of IEEE 802.11 which is responsible for medium access based on CSMA with Collision Avoidance (CSMA/CA) [39] [40].

3.1 Simulation procedure

Simulation procedure for proposed agent model is as follows:

Begin

1. Topology generation: Generate VANET in given road length by placing vehicles uniformly. Each vehicle maintains a data structure to store information as specified by scheme.
2. Apply mobility to nodes (vehicles).
3. Generate proposed agency (agents are implemented as objects).
4. Compute the performance of system.

End

3.2 Simulation Inputs

The simulation input parameters are as below:

Table 1. Simulation input parameters

Simulation parameters	Values
Network simulator	ns-2.34
Simulation time	Simulation time: 600 seconds
Simulation area	5000m X 5000m
Number of vehicles	50/100/150
Transmission range	150m/300m
Speed	Minimum: 20 Km/hr., Maximum: 40 and 60 Km/hr.
Data type	Constant Bit Rate
MAC protocol	IEEE 802.11e EDCA based DCF
Safety distance between vehicles	4 mts
Available bandwidth	5000 Mbps
Road type	Free way

3.3 Performance Parameters

1) *% of packets delivered:* Packet delivery ratio is the ratio of number of packets received at the destination node to the number of packets sent from the source node. The performance is better when packet delivery ratio is high.
2) *Route reliability:*The link reliability is defined as the stable duration of the communication link between two vehicles. Broken link is the link which disconnects while communication. If route has less disconnected links then the route is more stable. Otherwise, due to high disconnection of links there is more packet loss and more exchange of control packets.
3) *Route discovery time:* Route discovery time is the time difference between the VIMA of the source vehicle triggering the Destination path finder agent (DPFA) and DPFA updating the VKB of the source vehicle about the reliable route to the destination.
4) *Delay:* It is the time taken to transmit the data from the source vehicle to the destination vehicle.It is expressed in terms of milliseconds. It represents end-to-end delay which refers to the time taken for a packet to be transmitted across a network from source to destination.

IV. SIMULATION RESULTS AND ANALYSIS

This section presents the results obtained during simulation. We compare results of proposed work with an existing routing protocol AODV-L. The below mentioned figures are generated based on the simulation results.

% of Packet Delivery (Packet Delivery Ratio)

Figure 13 shows the Packet Delivery Ratio (PDR) evaluated for AODV-L and MSRR protocols by increasing the number of vehicles in the urban scenario. The PDR of MSRR is higher than AODV-L routing protocol. The PDR of MSRR is better when the vehicle density is more eventhough the average mobility of vehicles is more. MSRR protocol computes the reliable path having the highest trust value and higher reliability weight. This path is more reliable that results in better PDR.

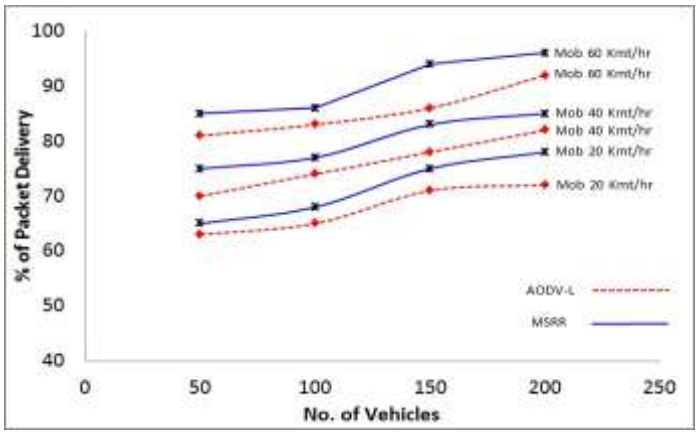

Figure 13. % of Packet Delivery v/s No. of vehicles

Route reliability

Figure 14 shows the variation in route reliability for both protocols AODV-L and MSRR. As the graph depicts the expected disconnection degree of links in the path for MSRR is fairly less than AODV-L which indicates more reliability of routes for MSRR protocol. This is because in MSRR the selected path will be of higher trust value and reliability weight.

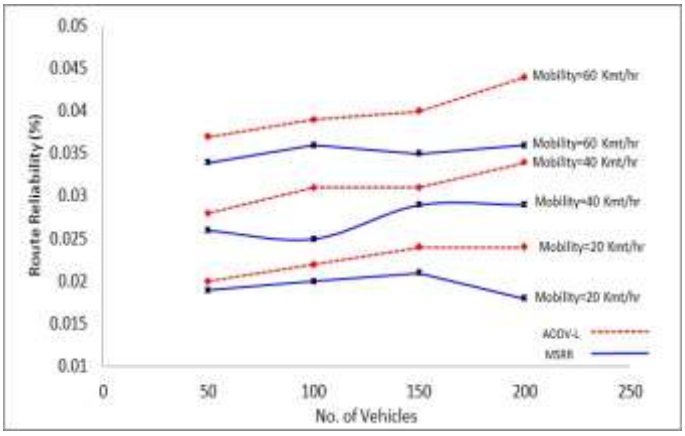

Figure14. Route reliability v/s No. of vehicles

Route Discovery time

Figure 15 shows variation of the route discovery time versus the number of vehicles with varying mobility of the vehicles. From the figure it is evident that there is considerable increase in route discovery time as the node density and node mobility is increased.Route discovery time taken by MSRR is lesser as compared to AODV-L because it uses the intelligent software agents for computation of the reliable and secured path.

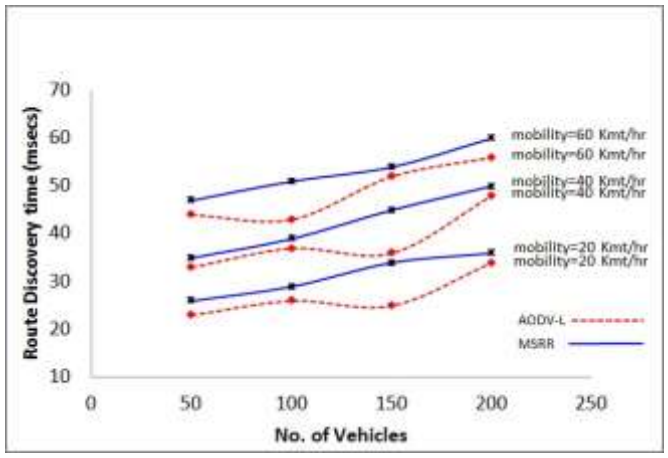

Figure15. Route Discovery time v/s No. of vehicles

Delay

Figure 16(a) shows the delay versus mobility with varying link failures. When the average speed of the vehicles increases vehicles needs to update its information in parent node and connected RSU, intern routes are computed using the fresh information, which consumes more time.

The Figure 16(b) presents the delay versus the number of vehicles with varying malicious nodes. When the number of vehicles increases, computation of the reliable paths takes more time. From the figure we notice that the delay substantially increases with the increase in number of malicious nodes. Delay introduced by MSRR as compared to AODV-L is lower. This is because of the mobile agentswhich in the process of generating reliable paths, migrate carrying partially integrated results whichleads to progressive accuracy.

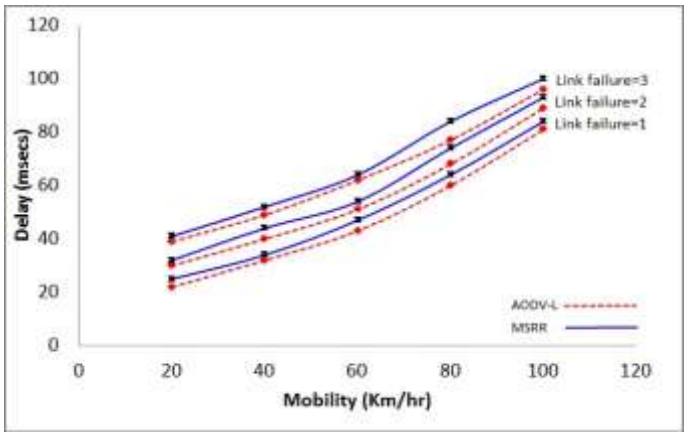

Figure16(a). Delay v/s mobility

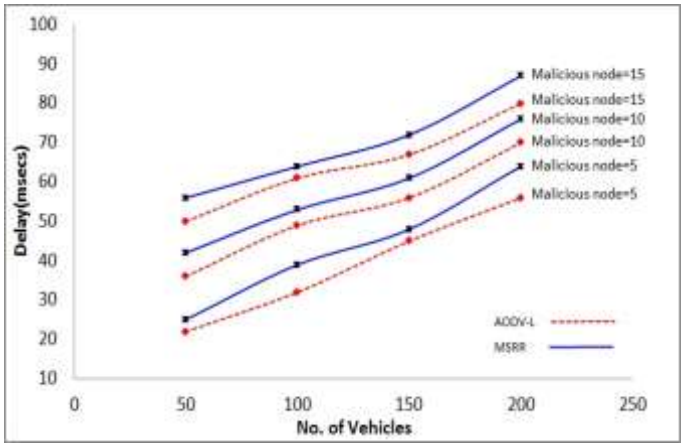

Figure16(b). Delay v/s No. of vehicles

V. CONCLUSION

The proposed scheme presented a multi-agent system based secured and reliable routing in VANET by employing a set of static and mobile agents. The source node activates the path discovery mechanism by calculating the favourable nodes in the direction of destination node dynamically.The proposed scheme used clones of mobile agents for traversing the path towards destination. Intermediate nodes on the path are selected based on neighbourhood information and trust value. Whenever two clones meet at any intermediate node best path is calculated based on the reliability weight. Thus the intermediate nodes on the discovered path are trustworthy and the path is reliable. The process of computing the path is

incremental and leads to progressive accuracy. As compared to AODV-L, the proposed MSRR performed better in terms of packet delivery ratio, route reliability, route discovery time and delay.

REFERENCES

[1]. Nizar Alsharif, Xuemin (Sherman) Shen, (2017) "iCAR-II: Infrastructure-based Connectivity Aware Routing in Vehicular Networks", IEEE Transactions on Vehicular Technology, Vol. 66, Issue 5, pp 4231 – 4244 .

[2]. Kapil Sharma, Brijesh Kumar Chaurasia , ShekharVerma and Geetam Singh, (2016) "Token Based Trust Computation in VANET ", International Journal of Grid and Distributed Computing Vol. 9, No. 5, pp 313-320.

[3]. Tasneem Darwish, Kamalrulnizam Abu Bakar, (2016) "Traffic aware routing in vehicular ad hoc networks: characteristics and challenges", Telecommunication Systems, Vol. 61, Issue 3, Springer, pp 489–513.

[4]. Mahmoud HashemEiza, Thomas Owens, and Qiang Ni, Senior Member, (2016) "Secure and Robust Multi-Constrained QoS aware Routing Algorithm for VANETs", IEEE Transactions on Dependable and Secure Computing , Vol. 13, Issue 1, pp 32-45.

[5]. Samira Harrabi ,Ben Jaafar ,KhaledGhedira ,(2016) " A Novel Clustering Algorithm Based on Agent Technology for VANET", Network Protocols and Algorithms, ISSN 1943-3581, Vol. 8, No. 2 (doi: 10.5296/npa.v8i2.8434)

[6]. Neha Goel, Isha Dhyani, Gaurav Sharma, "A Study of Position Based VANET Routing Protocols", In: Proceedings of IEEE International Conference on Computing, Communication and Automation, April 2016, India (doi: 10.1109/CCAA.2016.7813803).

[7]. T. Sivakumar, R. Manoharan, (2016) "SRP: A Stable Routing Protocol for VANETs", International Journal of Applied Engineering Research ISSN 0973-4562 Vol. 11, No. 5, pp 3499-3504.

[8]. Ahmed I. Saleh a,,Samah A. Gamel a, Khaled M. Abo-Al-Ez b, (2016) " Reliable Routing Protocol for Vehicular Ad hoc Networks", Computers and Electrical Engineering, Elsevier Ltd., (https://doi.org/10.1016/j.compeleceng.2016.11.011).

[9]. Chang Sang-woo and Lee Sang-sun, (2016) "A Routing Protocol for Urban Vehicular Multi-hop Data Delivery", Chinese Journal of Electronic Vol. 25, No.2, pp 348-356.

[10]. Lina Zhu, Changle Li, Bingbing Li, Xinbing Wang, Guoqiang Mao, (2016) "Geographic Routing in Multilevel Scenarios of Vehicular Ad Hoc Networks", IEEE Transactions on vehicular technology, Vol. 65, No. 9, pp 7740 – 7753.

[11]. JianShen , Chen Wang , Anxi Wang , Xingming Sun , SangmanMoh , Patrick C.K. Hung, (2016) "Organized topology based routing protocol in incompletely predictable ad-hoc networks" Computer Communication 99, Elsevier , Issue C, pp 107-118 (https:// doi.org/ 10.1016/ j.comcom. 2016.07.009).

[12]. Xuanxia Yao , Xinlei Zhang , HuanshengNing , Pengjian Li , (2016) "Using trust model to ensure reliable data acquisition in VANETs", Ad Hoc Networks, Elsevier, Vol. 55, pp 107–118.

[13]. He, Yang, WenjunXu, and Xuehong Lin , "A Stable Routing Protocol for Highway mobility over Vehicular Ad-hoc Networks." In: Proceedings of Vehicular Technology Conference (VTC Spring), IEEE, Glassgow, UK, May 2015 (doi: 10.1109/VTCSpring.2015.7145647).

[14]. Souaad Boussoufa-Lahlaha, Fouzi Semchedinea, Louiza Bouallouche-Medjkoune,(2015) "A position-based routing protocol for vehicular ad hoc networks in a city environment", In: Proceedings of the International Conference on Advanced Wireless, Information, and Communication Technologies, Procedia Computer Science 73 (2015) 102 – 108 (doi: 10.1016 /.procs. 2015.12.054).

[15]. FarhanaAnjum, V.D.Bondre, Ausaf Umar Khan, (2015) "Design of Single and Multipath Routing Protocol for Quality of Service (QoS) in VANET" In: Proceedings of the IEEE India International Conference on Communications and Signal Processing, April 2015 (doi: 10.1109/ ICCSP.2015.7322606).

[16]. Sergio M. Tornell, Carlos T. Calafate, Juan-Carlos Cano, and Pietro Manzoni, (2015) "DTN Protocols for Vehicular Networks: An Application Oriented Overview", IEEE Communication surveys & tutorials, Vol. 17, No. 2, pp 868 – 887.

[17]. Celimuge Wu, YushengJi, Fuqiang Liu , Satoshi Ohzahata , Toshihiko Kato, (2015) "Toward Practical and Intelligent Routing in Vehicular Ad Hoc Networks", IEEE Transactions on Vehicular Technology, Vol. 64, No 12, pp 5503-5519.

[18]. Amrita Jain, VivekKapoor, (2015) "Secure Communication using RSA Algorithm for Network Environment " , International Journal of Computer Applications (0975 – 8887) Vol. 118, No. 7, pp 6-9.

[19]. JacekRak, (2014) "LLA: A New Anypath Routing Scheme Providing Long Path Lifetime in VANETs", IEEE Communications letters, Vol. 18, No. 2, pp 281-284.

[20]. Samira Harrabi ,WalidChainbi,KhaledGhedira, (2014)" A Multi-Agent Proactive Routing Protocol for Vehicular Ad-Hoc Networks", In: Proceedings of International Symposium on Networks, Computers and Communications, Tunisia, July 2014 (doi: 10.1109 /SNCC. 2014. 6866523).

[21]. Ramesh B. Koti and Mahabaleshwar S. K., (2014) "Multi Agent Based Congestion Control in VANETs", International Journal of Future Computer and Communication, Vol. 3, No. 2, pp 102-104.

[22]. CarolinaTripp-Barba, Luis Urquiza-Aguiar, MonicaAguilarIgartua, David Rebollo-Monedero, Luis J.dela Cruz Llopis, Ahmad Mohamad Mezher and Jose Alfonso Aguilar-Calder, (2014) "A Multimetric, Map-Aware Routing Protocol for VANETs in Urban Areas ", Sensors, Vol. 14, No. 2 , pp 2199-2224.

[23]. Mayuri Pophali, Shraddha Mohod, T.S.Yengantiwar, (2014) "Trust Based Opportunistic Routing Protocol for VANET Communication", International Journal of Engineering And Computer Science,Vol. 3, Issue 8, pp 7408-7414.

[24]. Sourav Kumar Bhoi, Pabitra Mohan Khilar, (2014) "SIR: a secure and intelligent routing protocol for vehicular ad hoc network", IET, Vol. 4, No. 3, pp 185-194.

[25]. Pavlos Sermpezis, Georgios Koltsidas, and Fotini-Niovi Pavlidou, (2013) "Investigating a Junction-Based Multipath Source Routing Algorithm for VANETs", IEEE Communications letters, Vol. 17, No. 3, pp 600-603.

[26]. Mahmoud HashemEiza and QiangNi , (2013) "An Evolving Graph-Based Reliable Routing Scheme for VANETs", IEEE Transactions on Vehicular Technology, Vol. 62, No. 4, pp 1493-1504.

[27]. Dr A.V. Sutagundar, Dr S SManvi, (2013) "Location aware event driven multipath routing in Wireless Sensor Networks: Agent based approach", Egyptian Informatics Journal, Vol. 14, No. 1, pp 55–65.

[28]. Mahmoud HashemEiza, Qiang Ni , Thomas Owens and Geyong Min , (2013) "Investigation of routing reliability of vehicular ad hoc networks" EURASIP Journal on Wireless Communications and Networking (doi:10.1186/1687-1499-2013-179).

[29]. Nentawe Y. Goshwe,(2013) "Data Encryption and Decryption Using RSA Algorithm in a Network Environment " ,IJCSNS International Journal of Computer Science and Network Security, Vol.13, No.7, pp 9-13.

[30]. M. J. Khabbaz, W. F. Fawaz, and C. M. Assi,(2012) "Modeling and delay analysis of intermittently connected roadside communication networks," IEEE Transactions on Vehicular Technology, Vol. 61, No. 6, pp 2698–2706.

[31]. Oscar Urra, Sergio Ilarri, Thierry Delot and Eduardo Mena "Mobile Agents in Vehicular Networks:Taking a First Ride", In: Proceedings of International Conference on Practical Applications of Agents and Multiagent Systems , 2010 (doi: 10.1007/978-3-642-12384-9).

[32]. Network simulator: ns-2, Available: http://www.isi.edu/nsnam/ns [October 2010].

[33]. JosianeNzouonta, NeerajRajgure, Guiling Wang, (2009) "VANET Routing on City Roads using Real-Time Vehicular Traffic

Information", IEEE Transactions on Vehicular Technology,Vol. 58, No. 7, pp 3609 – 3626.
[34]. Fan Li and Yu Wang, University of North Carolina at Charlotte,(2007) "Routing in Vehicular Ad Hoc Networks: A Survey", IEEE Vehicular Technology , Vol. 2, Issue 2, pp 12 – 22.
[35]. Tarik Taleb, Kazuo Hashimoto, (2007) " A Stable Routing Protocol to Support ITS Services in VANET Networks", IEEE Transactions on vehicular technology, Vol. 56, No. 6, 3337 – 3347.
[36]. Charles Harsch , Andreas Festag, PanosPapadimitratos, "Secure Position-Based Routing for VANETs, In: Proceedings of IEEE 66th Vehicular Technology Conference, USA, October 2007 (doi: 10.1109/VETECF.2007.22).
[37]. Bangalore City Map, Available: www.mapofbangalore.com [November 2007].
[38]. Tarik Taleb, Mitsuru Ochi, Abbas Jamalipour, Nei Kato, and Yoshiaki Nemoto ,"An Efficient Vehicle-Heading Based Routing Protocol for VANET Networks", In:Proceedings of IEEE Wireless Communications and Networking Conference, April 2006 (10.1109/ WCNC. 2006. 1696637).
[39]. W. Xiuchao and A. L. Ananda, "Link Characteristics Estimation for IEEE 802.11 DCF based WLAN", In: Proceedings of IEEE International Conference on Local Computer Networks, Tampa, USA, November 2004 (doi: 10.1109/LCN.2004.73).
[40]. S. Wiethlter and C. Hoene, "Design and Verification of an IEEE 802.11e EDCF Simulation Model in NS-2.26", Technical report, Telecommunication Networks Group, Technische, Universitt Berlin, November 2004.
[41]. F. Bai, N. Sadagopan, and A. Helmy, "Important: A Framework to SystematicallyAnalyze The Impact of Mobility On Performance of Routing Protocols for Ad hocNetworks", In: Proceedings of 22th IEEE Annual Joint Conference on Computer Communicationsand Networking, April 2003 (doi: 10.1109/INFCOM.2003.1208920).
[42]. Rivest R, Shamir A, Aldeman L, "A method for obtaining Digital Signatures and Public-key Cryptosystems", Communications of the ACM, 21(2): 120-126, February 1978 (doi:10.1145/ 359340.359342).

AUTHORS

Anil D. Devangavi completed his B. E in Computer Science and Engineering from Karnatak University Dharwad, India and M. Tech from Visvesvaraya Technological University Belgaum, India. He is pursuing Ph. D in the area of Vehicular Adhoc Networks (VANETs) from AISECT University, Bhopal, India. Presently, he is working as Associate Professor in Department of Information Science and Engineering, Basaveshwar Engineering College, Bagalkot, Karnataka, India. He has published 3 international journal papers. His areas of interest are wireless network and VANETs.

Dr. Rajendra Gupta is Assistant Professor in AISECT University, Raisen. He is doctorate in Computer Science and having 18 years of working experiences in Government and Non-Government Sectors. His teaching and research areas belong to Networking, Network Security, Data Mining, Statistical Analysis and Computer Graphics and Multimedia. He has published 22 research papers in International and National Journals and completed a UGC minor research project. He has designed four SLM for MP Bhoj University, Bhopal on the topic of 'Computer Organisation and Architecture', 'Data Communication and Computer Networks', 'Software Engineering' and 'Operating System'. He is reviewer of two International Journals and member of Academic Body.