QoS Swarm Bee Routing Protocol for Vehicular Ad Hoc Networks

Salim Bitam
Computer Science Department
Mohamed Khider University
Biskra, ALGERIA
salim.bitam@laposte.net

Abdelhamid Mellouk
Image, Signal and Intelligent Systems Laboratory-LISSI
Dept. of Networks and Telecoms, IUT C/V
University of Paris Est Creteil (UPEC), FRANCE
mellouk@u-pec.fr

Abstract—Research and industries are recently more interesting and attracting to the Vehicular Ad hoc Networks (VANETs) development domain. They contribute to safer and more efficient roads by providing timely and accuracy information to drivers and authorities. Thus, the definition of a quality of service routing protocol for VANETs is one of their challenges. In this paper, we propose QoS BeeVanet, a new quality of service multipath routing protocol adapted for the vehicular ad hoc networks. It is based on ideas of the autonomic bee communication. Simulation results taken with NS2 in realist urban settings were shown that QoS BeeVanet outperforms DSDV and AODV two of the current state-of-the-art protocols, in terms of end-to-end delay, packet delivery ratio, and normalized overhead load.

Key words— Vehicular ad hoc network; Adaptive multipath routing; Swarm bee communication; QoS;

I. INTRODUCTION

In the last decade, the scientific community trends to study Vehicular Ad hoc Network which is considered as very active field of research and development. One goal is to increase road safety and comfort for passengers in order to avoid accidents and traffic congestion [1]. VANET represents a special kind of mobile ad hoc network. It aims to provide communications among vehicles via Inter-Vehicle Communication and between vehicles and fixed equipments described as roadside base stations via Roadside-to-Vehicle Communication such as the Internet access points which can be found along the road. It is distributed, adaptive network, characterized by very high node mobility, high speed variation of vehicles, and limited degrees of freedom in the mobility patterns. This situation leads to very fast and very frequent change of network topology [2].

In this field, one of the most important requirements is the quality of service that provides information needed in time to passengers in order to make safe decisions. Technically, QoS guarantees are of a special importance in delivering messages with minimum end-to-end delay. In this context, the following problem is a development issue: when communication endpoints are not within their respective ratio transmission range, how is it possible to establish communication between two vehicles or between vehicle and a roadside base station within QoS conditions?

Several potential research works have been investigated widely in VANET routing protocols which fall into two major categories: topology-based and geographic routing protocols [3]. They will be explained in the next section.

In this work, we present a new quality of service multipath routing protocol called QoS BeeVanet for VANET considered as a topology-based algorithm. It is based on biological paradigm of communication between bees in the food source searching behavior. It is seen as reactive, self-configured and distributed protocol which uses a special type of transmission called stochastic broadcasting in its route discovery defined in [4]. In the aim to validate its guaranty of the QoS requirements, simulation experiments of the proposed protocol are carried out in NS2 followed by a comparison against DSDV and AODV protocols in terms of QoS metrics.

The organization of the rest of this paper is as follows. Section II overviews the topology-based routing and geographic routing as related works. In section III, we describe the QoS BeeVanet routing protocol. Section IV is devoted to NS2 simulations and experimental results. Finally, section V concludes the paper and highlights ideas for future work.

II. RELATED WORKS

After an analysis study of the proposed protocols to the VANETs, two main categories can be distinguished: topology-based routing protocols category and geographic routing category.

A. Topology-based routing category

The topology-based routing protocols have been proposed for the MANETs field. The creation of topological end-to-end paths is the common principle among these protocols. They can be reactive or proactive. The most MANET routing protocols are applied to the VANET, such as Destination-Sequenced Distance-Vector protocol (DSDV) [5], Ad hoc On-demand Distance Vector (AODV) [6] and Dynamic Source Routing protocol (DSR) [7]. Nevertheless, we can distinguish VANET from MANET by its highly dynamic topology due to the frequent mobility. In this way, studies based on simulations which have been done to evaluate the performance of VANET routing protocols in various traffic conditions showed that many mobile ad hoc routing protocols exploit poorly the
bandwidth and tend to have poor route convergence. Consequently, it is necessary to adapt and modify these protocols to deal with the VANET properties or to develop new routing protocols for this category [8].

B. Geographic routing category

In geographic routing protocols, the source node sends a packet to the geographic position of the destination instead of sending it to the destination address. MAINLY, source node can determine the position of the node’s one hop neighbors which is obtained by hello packets sent periodically. Moreover, the destination location is known by the source node. Thus, it can make its forwarding decision. We can mention the following examples of geographic routing approaches: Greedy Perimeter Stateless Routing (GPSR) [9] and Greedy Perimeter Coordinator Routing (GPCR) [10]. To forward packets towards the destination, GPSR and GPCR use greedy algorithms in order to select the best relays. They can use a recovery mode in case such solutions fail. These protocols are very efficient if the node population is dense and thus the underlying topology is well connected. The major drawback of such protocols is the tendency to introduce partitions and disconnections due to the VANET properties which are the vehicle mobility and radio obstacles.

III. QoSBeeVanet protocol

In this section, the proposed routing protocol for VANETs will be presented. We start with a brief explanation of the bee communication phenomenon which represents some basic idea of the protocol. After that, a projection of this phenomenon on the QoS routing process for VANETs is initiated. Furthermore, QoSBeeVanet principle is presented, and followed by a description of their different phases.

A. Bees communication principale

The bees are domestic insects live in colony which is divided in a single breeding female (Queen), a few thousands of males (Drones), a several thousands of sterile females (Workers), and many young bee larvae (Broods). They share a communication language based on dances which are performed by the worker called “Scout” when it finds food. This dance aims to recruit others by the transmission of the distance, direction and quantity of found food with a visual, tactile and olfactory perception. Thus, some bees are recruited and then, become “foragers”. Their number is proportional to the found food quantity. This phase is called the exploitation phase. In the exploitation step, bee collects food and calculates its quantity to make a new decision. Either, it continues collecting by memorization of this best location or it leaves the food and returns to the beehive as simple bee [11].

B. Adaptation to QoSBeeVanet conditions

QoSBeeVanet protocol is inspired by communication in swarm of bees. A native version has been applied to MANET and proved in [4]. A projection in the VANET area is required to deal with the VANET features. First, beehive is seen as the end-point sender such as vehicle. The destination which may be vehicle or roadside base station corresponds to the bees’ food source. Intermediate vehicles or roadside base stations are represented by workers. Each entity possesses its own routes table which contains the different paths to the desired destination. Only the next hop for the destination is indicated.

C. QoSBeeVanet packet types

Scout and forager are the two major kinds of packets used in the protocol. It employs periodically a refresh packet to update the immediate neighbor list of the node (vehicle or roadside base station) and the available QoS information. A node is considered as immediate neighbor if it appears in the transmission range of the current node. For the route maintenance, an error scout packet is used to warn the concerned nodes. It will be launched when a link is broken or when a QoS requirements are violated.

1) Scout

This control packet is used in the route request. First, it is called forward scout until finding the food (destination). Thus, it returns to the beehive (source node) to inform its nest mates (data packets). In the backway, it’s named backward scout.

a) Forward scout

It ensures the exploration of the VANET in order to find the destination. It is launched from the source node to nodes in neighborhood and so on until finding the destination. It marks temporarily its itinerary in the routes tables of the visited nodes in order to be used on the backway. A forward’s scout identifier is unique; in fact, it’s constructed as an incremental value. Forward scout includes also the beehive identifier. A unique identification of the route request is represented by the conjunction of these last two identifiers. It prevents the route request duplication.

This control packet contains also the food identifier, the minimum bandwidth requested and the maximum delay allowed by the source node, and a lifespan field used to limit number of hops to be done by the packet. Thus, if reached, the forward scout will be dropped. It ensures the loop-free propriety of the route request. Note that lifespan field will be increased if the beehive doesn’t receive any response after the waiting time expiration. Forward scout records a hop count field which is the number of hops carried out from the source node to the node handling this scout. In addition, it includes stamp field used to save the transmission time which employs to compute available bandwidth and measured delay and then to decide if the network satisfy the QoS guarantees.

b) Backward scout

Once the route is found, the node propagates the scout in backward scout form toward the source node along the reverse path. Backward scout includes the same fields as forward scout such as: the scout identifier, the beehive identifier, the food identifier, the minimum bandwidth requested and the maximum delay allowed by the source node. Backward scout employs the hop count field in order to indicate number of hops from the source node to the destination. This field is initialized using the hop count field of the forward scout when finding the desired route. Furthermore, the stamp field is used to inform the source node by the bandwidth and the delay carried out between the source node and the destination. It contains the trip
time estimated by the forward scout. Backward scout takes advantage of lifespan field as a time to live field. It represents the time validity of the route in the backward scout trip.

2) Forager

This packet type represents data packet used to transmit the communication data. Data packets are queued until the discovery process of the desired route is terminated, and then they will be launched to the destination.

D. Routes table

Each node possesses its own routes table which contains the different routes toward known destination nodes. For each destination, multiple paths may be recorded in the table. Each path is evaluated relevant to its quality by a weighting factor. If the path possesses the important weighting factor, it will be used to transport more packets than the others. Hence, each weighted route is represented by one entry which contains the following fields “fig. 1”: the food identifier, the identifier of next hop node toward this destination and the identifier of prior hop greates to the source node. The next hop field is used to transmit data packets and the prior hop field warns an eventual link update in the communication range of the current node to the benefit of its prior nodes until arriving to the source node. Note that the link update cases are either change in available bandwidth or estimated delay between nodes or connection failure in links. They can be detected using refresh packets. The routes table entry includes also, hop count field which indicates the number of hops to reach the destination and weighted factor field related to the route quality. It is calculated according to the delay taken by the transmitted packet via this route. The greater weighted route value is given to the route with the lower delay and so on.

The scout identifier is one of the fields of the routes table entry. It is temporarily saved when the forward scout executes the route request until finding the destination. Hence, it will be permanently recorded by the backward scout. This field corresponds to the novelty of the new route. In addition, a timeout field is used to retransmit a new forward scout if the former doesn’t return after passing this waiting time. For each entry, the average end-to-end delay and bandwidth between the source node and the destination are saved. There are calculated using the stamp field included in the forward scout packet. A route is considered valid in the routes table except if the QoS guarantees are not be satisfied or if there is a link failure in the route. Also, immediate neighbors list is recorded for each node.

E. QoSbeeVanet pertinent description

1) Neighborhood connection discovery phase

In this phase, each node informs its neighbors that the links are active. Also, it aims to refresh these connections by the estimation of the available bandwidth and the measured delay of each link used for the QoS requirements. All nodes in the VANET broadcast a refresh packet periodically with its immediate neighbors. When a neighbor node receives the refresh packet, all route entries in its routes table regarding the sender will be consider as valid. In addition, the available bandwidth and the measured delay of the link will be saving in the relevant fields of the routes table entry. If the node does not get information from the node’s neighbor for specified amount of time, then the routing information in the routes table is marked as lost. In this case, the bandwidth and delay of the relevant entry will take the infinity value. Hence, an error scout packet is generated and sent to inform others of the link breakage.

2) Route discovery phase

When one node is responsible to transmit data, it first checks whether the route is present in its routes table and the QoS requirements are satisfied. If checks if the bandwidth required by the application can be less than the bandwidth available for the route in its routes table. It checks also, if the delay allowed is greater than the possible delay which can be carried out by the transmission. If this is a case and there is a sufficient forgers, the source node transmits the data. If there is no forager, data wait recruiting foragers. In the case of no QoS route exists, bee hive generates and clones several forward scouts from one and unique forward scout. It launches and broadcasts them stochastically to its immediate neighbors. Stochastic broadcasting means the transmission of forward scouts to a limit percentage of neighbor nodes. In this work, an experimental value equal to 80% is chosen that leads to better results.

The cloned forward scouts have the same scout identifier, the bee hive identifier, the food identifier and the maximum lifespan of the route request. They record an hop count which is initialized with zero value and incremented while encountering each node until discovering the route. Every time the forward scout visits one node, the transport time is recorded by accumulation in the stamp field. Consequently, the current node checks the QoS validity and thus, the route discovery is continued, else the exploration is denied and the forward scout will be dropped.

The intermediate node checks also, if it has already received a forward scout with that same scout identifier and bee hive identifier. If it is the case the forward scout will be dropped, otherwise current node records in the routes table entry the forward scout identifier and the source node identifier at the prior hop field. It prevents a future treatment of the same scout. After that, the intermediate node checks the route existence in its routes table. As it is not the case, current node rebroadcasts stochastically the forward scout in the same manner such as the source node. If the intermediate node knows the route, it sends a backward scout to the source node along the reverse path. This is done by looking at the prior hop field at the routes table.
In return, the backward scout records the next hop at the tables route entry to indicate its sender. After the backward scout arrives at the source node, the link weight is calculated and recorded at the routes table entry using the stamp field. Now, the source node recruits a number of forager according to the quality of the route discovered. Consequently, waiting data are sending using foragers. Note that the routes are selected to transmit simultaneous data according to the link weight factor. This will reduce the network congestion and then, increases the bandwidth and decreases the delay. The following diagrams “fig. 2” explain the route discovery phase.

3) Route maintenance phase
To maintain connections in VANET, QoSBeeVanet performs as follows. The periodic sending of refresh packet between node and its neighbors ensures the stability of connections. It ensures also, the links safely in the transmission range of node. Otherwise, the node detects a link breaks and, then, any route passing this broken link is considered disconnected. Besides, the node can detect a QoS requirements violation (bandwidth insufficiency or large delay). In these cases, the detector node of this failure sends an error scout to the source node via the prior hop and so on. The goal here is to inform any node in the reverse route about the broken link to remove it from its routes table and to rediscover a new QoS route by the source node if needed.

IV. SIMULATION AND RESULTS
In order to evaluate QoSBeeVanet protocol in terms of end-to-end delay, packet delivery ratio and normalized overhead load, a set of simulations has been carried out. Furthermore, comparisons against DSDV and AODV have been conducted.

A. A realistic propagation model for VANET
Many VANET research activities use the network simulator NS2 in its native form to evaluate different routing protocols. However, it is known that NS2 simulates city traffics and vehicle movements in a theoretical form. VANET should be simulated according to realistic traffic models which are a complex challenge due to the urban traffic features such as the limit capacity of the roads and the existence of intersections, obstacles, buildings, etc. In this way, a realistic vehicular propagation model has been used in our experiments which defined taking into account real places located in Málaga city in Spain which uses only mobile nodes [12]. A scenario where there are thirty (30) vehicles moving through their roads has been employed. We have improved this scenario by adding eight (8) roadside stations to make it more realistic “fig.3”.

B. Simulation environment
We simulated QoSBeeVanet on the Ubuntu 9.10 Linux Operating System using network simulator NS2 in its version 2.34. The simulated network consisted of thirty (30) vehicles positioned according to the propagation model generated for Málaga city in terms of vehicle positions and movement [12]. Eight (8) roadside base stations have been positioned in different and fixed places “fig. 3”. The proposed simulation time is for 600 seconds in a 600 x 400 square meter area.
Fifteen (15) vehicles are considered as source nodes and the rest represent the destination nodes.

C. Significant results

To analyze performances of our proposal, three metrics have been considered. Average end-to-end delay (E-to-E Delay) includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, propagation and transfer times. Packet Delivery Ratio metric (PDR) is calculated by dividing the number of packets received by the destination node through the number of packets originated by the application layer of the source nodes. The last metric is the Normalized Overhead Load (NOL) which represents the total number of routing packets divided by total number of delivered data packets. It indicates the extra bandwidth consumed by overhead to deliver data traffic. We obtain the following results:

<table>
<thead>
<tr>
<th>TABLE I. SIMULATION RESULTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-to-E Delay</td>
</tr>
<tr>
<td>QoSBeeVanet</td>
</tr>
<tr>
<td>DSDV</td>
</tr>
<tr>
<td>AODV</td>
</tr>
</tbody>
</table>

D. Discussion

Simulation shows that QoSBeeVanet outperforms DSDV and AODV in terms of average end-to-end delay. It carries out just 0.15s compared to DSDV and AODV which have reached 1.02s and 1.10s respectively. A detailed analysis of this improvement proves that the proposed protocol ensures packet exchanges with a minor delay due to its multipath connectivity. This metric value shows the suitability of QoSBeeVanet to the QoS requirements which are a very important parameter in this vital field. The problem of DSDV protocol appears in its policy which is based on the periodic updating of each node routes table. It leads to an additional process with more control packet transmissions and then, it makes an additional time. In this case, packets arrive in an expired time. In the other hand, AODV presents the worst end-to-end delay value due to the processing time during the route request. Moreover, both of DSDV and AODV do not use the multipath principle which can reduce the transmission delay.

The observed packet delivery ratio values for the QoSBeeVanet protocol show the good delivery of packets with 98.74% as the best value after comparing with the other protocols. This metric presents one of the most important challenges of the VANETs which are exposed to a special condition in contrast to MANETs such as the presence of obstacles and the rapid change of the network topology. The metric is considered as one of the most drawbacks of the geographic routing protocols proposed for VANETs. The best value of our protocol is the result of multipath principle which guarantees many paths to the destination. Therefore, it helps to avoid the lost of packets caused by the congestion. We can see in table 1 an acceptable packet delivery ratio values for both DSDV and AODV. If we now take a look at the normalized overhead load, one can see that QoSBeeVanet provides an acceptable value 64.01% which is close to the AODV value 59.80%. These values change according to the network topology due the fact that these two protocols are reactive. On the other side, DSDV provides the best value (51.17%) which is not far from others.

V. Conclusion

In this paper, we proposed a new QoSBeeVanet protocol. It focuses on a quality of service routing protocol suitable to the vehicular ad hoc networks. It is reactive, distributed and topology-based protocol. We demonstrated by simulation study in a realistic propagation model that QoSBeeVanet outperforms the standard proactive and reactive routing protocols DSDV and AODV in terms of end-to-end delay and packet delivery ratio. In addition, it provides an acceptable normalized overhead load measure. The obtained results have been shown that the proposed protocol is more adequate to the transmissions in realistic vehicular networks which require the QoS guarantees compared to DSDV and AODV. As a future work, we would like to use QoSBeeVanet protocol across hybrid networks to achieve end-to-end QoS needs to be investigated, in particular on very large scalable VANETs.

REFERENCES