

# Routing and the Impact of Group Mobility Model in VANETs

Raad S. Al-Qassas

Department of Computer Science, Princess Sumaya University for Technology,  
P.O. Box 1438 Amman 11941 Jordan

## Article history

Received: 22-02-2016

Revised: 28-04-2016

Accepted: 14-05-2016

Email: raad@psut.edu.jo

**Abstract:** Group vehicular applications could play a vital role in our life, whether these applications are safety-oriented or convenience-oriented applications. The group concept has also been used in support of many solutions in VANETs. Reference Point Group Mobility model (RPGM) is a popular group mobility model and has been used heavily in the literature. In order to study the impact of this mobility model on routing in VANETs, two well-known protocols are considered, namely AODV and AOMDV, as representatives of single-path and multipath routing, respectively. These protocols have shown performance merits over other routing protocols and they have a vital role in other wireless networks including MANETs and Wireless Mesh Networks. This paper provides a thorough evaluation of these protocols, by examining them under various potential realistic scenarios, under the RPGM mobility model. To the best of knowledge, this is the first study that examines the behaviour of the two protocols under the RPGM mobility model. The results from extensive simulations have shown that both protocols have comparable performance merits when the number of communicating nodes is low. However, increasing the number of communicating nodes has demonstrated a performance advantage for AOMDV, in the majority of the performance metrics used in the paper.

**Keywords:** VANET, RPGM, AOMDV, AODV, Routing, Group Concept, Group-Oriented Applications

## Introduction

Wireless technologies are playing an important role in our lives. The advances in these technologies have been the trigger to provide various technological solutions at various operational levels that facilitate our lives. These technologies can support applications not only for local and wide area networks, but also for body and personal area networks. Vehicular Ad Hoc Network (VANET) is an example of the promising wireless networks. A VANET is a self-organized network that can be formed without the need of any centralized control. The nodes in the network may act as routers and play a key role in establishing and maintaining routes between communicating nodes. Vehicles in VANET can communicate with each other directly forming what is known as Vehicle to Vehicle (V2V) communication (Al-Sultan *et al.*, 2014), or can communicate with Road Side Units (RSUs) forming Vehicle to Infrastructure (V2I) communication (Grover *et al.*, 2012). The communication is established

between vehicles based on the Dedicated Short Range Communication (DSRC) which utilizes the IEEE 802.11p (Gerla and Kleinrock, 2011). The IEEE 802.11p standard is also called WAVE which stands for Wireless Access in Vehicular Environments.

VANETs have gained a lot of attraction in the past few years (Gerla and Kleinrock, 2011; Mejri *et al.*, 2014; Al-Sultan *et al.*, 2014; Thenmozhi and Govindarajan, 2016; Hager *et al.*, 2015; Whaiduzzaman *et al.*, 2014). A lot of challenges accompanied this hot area of research, these challenges are associated with various factors including highly dynamic topology caused by the high mobility and malicious communication disturbance. These factors can greatly affect the performance of the network (Ahmed *et al.*, 2014; Moravejosharieh *et al.*, 2013; Anggoro *et al.*, 2012).

The VANET promising applications can be categorised into safety and non-safety applications (Gerla and Kleinrock, 2011; Engoulou *et al.*, 2014). Safety applications can be represented in traffic control, disaster recovery and hazards prevention

applications. Non-safety applications can be represented in road service information and group communication applications.

Extensive research efforts have been conducted in the study and development of VANET at various levels including the routing level. The routing protocols AODV and AOMDV have been the focal of many research studies in VANETs (Anggoro *et al.*, 2012; Yufeng *et al.*, 2009; Dhilipkumar *et al.*, 2013; Sakthi Ganesh and Venkata Krishna, 2013; Ravi and Praveen, 2014; Kabir *et al.*, 2015; Arulkumar and Raj, 2015) because of their performance merits over other routing protocols. Mobility models are crucial part in investigating the performance of routing protocols. The mobility model is responsible for producing the network topology and how it may change. It determines the frequency of topology changes and the behaviour of nodes in the network in terms of mobility patterns. The impact of Reference Point Group Mobility (RPGM) model plays an important role in the evaluation of routing protocols for wireless networks (Amjad, 2011; Jiajia *et al.*, 2015; Verma *et al.*, 2013; Xi *et al.*, 2014; Simaremare *et al.*, 2013). This mobility model is ideal to represent groups of vehicles moving around. Furthermore, the group concept is employed in many studies including security and privacy solutions (Sampigethaya *et al.*, 2007; Weerasinghe *et al.*, 2010).

There have been a number of studies (Moravejosharieh *et al.*, 2013; Anggoro *et al.*, 2012; Vidhale and Dorle, 2011; Nagaraj and Dhamal, 2012; Al-Qassas, 2015) that compare the performance of these protocols under various mobility models. However, to the best of knowledge, this is the first study that evaluates and compares the performance of AODV and AOMDV under the RPGM model, in order to show their trade-off to allow researchers to select the most appropriate protocol for their ongoing research work. This paper conducts thorough simulation experiments to evaluate these protocols and show their applicability.

The performance merits is captured using general efficiency measures like throughput and end-to-end delay, in addition to other measures including normalised average load, normalised routing overhead and normalised end-to-end delay. The normalised average load is used as a measure to capture the protocols ability in distributing the traffic load over nodes. The normalised routing overhead and the normalised average load are important to show the ability of the routing protocol in saving resources. While the normalised end-to-end delay provides better understanding of the achieved end-to-end delay as it considers the amount of received data.

The rest of this paper is organized as follows. Section 2 describes the operations in AODV. Section 3 describes the operations in AOMDV. Section 4 illustrates the

Reference Point Group Mobility model. Section 5 describes the simulation environment. Section 6 presents the performance evaluation of AODV and AOMDV through conducting extensive simulation experiments. Finally, section 7 concludes the work.

## Ad Hoc On-Demand Distance Vector (AODV)

AODV (Perkins *et al.*, 2003) is an on-demand reactive protocol that establishes routes as needed. The protocol is designed to reduce the number of required flooding operations for route discovery. The operation of AODV consists of two processes: *Route discovery* and *route maintenance*.

### Route Discovery

When a source node needs to send data to another node, a route discovery process is initiated in order to establish a path between the source node and the destination node. The source node broadcasts a *route request* packet to its neighbouring nodes. Each node receives a route request copy will broadcast it to its neighbouring nodes. This process continues until the route request reaches the destination node. Each node that forwards a route request creates a *reverse route* back to the source node itself. Because of the broadcast nature of route requests, duplicate copies that arrive later are discarded. When the route request arrives at the destination, a special packet known as *route reply* packet is unicasted to the source node. The route reply packet travels to the source node through the reverse route that was created as the route request propagated in the network. The nodes that participate in forwarding the route reply packet back to the source node, add in their routing table a *forward route* to the destination node. It is worth to note that nodes along the formed path are not required to know about which nodes are forming the path. Each node stores the next hop rather than the entire path.

AODV utilizes a *sequence number* as an indication of route information freshness. In order to ensure that the used routes are up-to-date and loop-free, AODV uses the destination's *sequence number*. The source node embeds the last known sequence number of the destination node in the route request. An intermediate node that has a fresh route to the destination i.e., if it has a higher destination sequence number than the one in the route request packet, can respond to the route request.

### Route Maintenance

When an intermediate node along the path to the destination, discovers that an active route is broken, it initiates a route maintenance process. This may happen when the next node along the path becomes unreachable.

In this case, the node updates its routing table by removing the associated routing entry from the table and then it sends a *route error* packet to the affected neighbouring nodes that are actively using that route; to inform them that the route is no longer available. Therefore, AODV utilizes an active neighbours list to track nodes that are using a particular route. The route error packet keeps propagating until it eventually reaches the affected source nodes, which in turn can initiate a new route discovery process if needed.

## Ad Hoc On-Demand Multipath Distance Vector Routing (AOMDV)

AOMDV (Marina and Das, 2001) has been developed as a reactive multipath protocol based on AODV protocol. Of the important features in AOMDV is that it guarantees loop freedom and disjointness of the generated paths. The disjointness of the routes is computed without the use of *source routing* (Perlman, 1992). The operation of AOMDV protocol consists of two processes: *Route discovery* and *route maintenance*.

### Route Discovery

Similar to AODV, route discovery process is initiated when a source node needs to establish a path to a destination node. However, unlike AODV, a route discovery process is capable to establish more than one route to the destination node. The source broadcasts a *route request* packet to its neighbouring nodes. Each node receives a route request copy will broadcast it to its neighbouring nodes. This process continues until the route request reaches the destination node. In order to be able to form alternative routes, the route request duplicate copies that arrive later are not discarded until they are examined for potential alternative routes. Only the copies that meet with the loop-freedom and link disjointness criteria described in (Marina and Das, 2001) will be used to form the reverse routes.

For each route request copy received, the intermediate node checks if it has one or more valid forward routes to the destination node that have not been used in any previous route replies for this specific route request. If so, a *route reply* is sent to the source node along the reverse path. Otherwise, the intermediate node will forward the route request if it has not been previously forwarded. When the route request copies reach the destination node, reverse routes will be formed in the same way as in intermediate nodes. However, a route reply is generated in response to every route request copy that arrives via a loop-free route.

### Route Maintenance

A route maintenance process is triggered when all paths to a given destination are no longer available. To

declare a route failure, AOMDV uses a *route error* packet. The node that detects the failure generates a route error packet and sends it to the affected source nodes. As the route error packet propagates to the affected nodes, each node will remove the route entry from its routing table. When a source node receives the route error packet, it removes the route entry from its routing table and initiate a new route discovery process or to stop sending data to the destination.

## Reference Point Group Mobility Model

Reference Point Group Mobility Model (RPGM) (Jayakumar and Ganapathi, 2008; Aschenbruck *et al.*, 2010) is a popular mobility model that has been the focus of many recent studies. RPGM employs group behaviour to simulate the nodes mobility, where nodes move in groups. Each group has a group leader and the other nodes in the group move randomly around this group leader, considering it as their reference point, which makes them move in the same direction of the group leader. Of course, each node can have its own direction and speed, however they are derived from the direction and speed of the group leader. The importance of group mobility models is that it simulates real-life scenarios such as Sahara trips, army based vehicles' movement, disaster recovery rescue crews, etc.

The group leader movement at time  $t$  is defined using a motion vector  $V$ . The group members follow the motion of the group leader by some deviation degree. The group leader motion follows the random waypoint model (Lin *et al.*, 2004). The allowed distance deviation from group leader follows uniform distribution with interval  $(0, r]$  where  $r$  is the maximum allowed distance deviation, with uniformly distributed direction. Equations 1 and 2 characterise the movement of group members. The deviation from group leader is symbolised in two parameters: The Speed Deviation Ratio (SDR) and Angle Deviation Ratio (ADR) to form the speed and direction of group member relative to the group leader. Where  $V_i^t$  represents the speed vector for group member  $i$  at time  $t$ ,  $V_l^t$  represents the speed vector for group leader  $l$  at time  $t$ ,  $S$  represent the maximum speed,  $Direction_i^t$  represents the direction vector for group member  $i$  at time  $t$ , whereas  $Direction_l^t$  represents the direction vector for group leader  $l$  at time  $t$  and  $A$  represents the angle. Both SDR and ADR should have a value between 0 and 1:

$$V_i^t = V_l^t + \text{random}() * \text{SDR} * S \quad (1)$$

$$Direction_i^t = Direction_l^t + \text{rendom}() * \text{ADR} * A \quad (2)$$

Various mobility patterns can be simulated using RPGM. This includes in-place mobility, overlap mobility and convention mobility. In the in-place mobility scenarios the simulated area is divided into regions, each group occupies a single region. In the overlap mobility scenarios, the groups move in an overlapping manner. Where as in the convention mobility scenarios, some of the groups can move between the regions.

## Simulation Environment

### Simulation Model

In order to conduct simulation experiments the well-known ns-2 simulator has been used. This simulator is a proven simulation tool that has been used extensively in the area of wireless networks (Arulkumar and Raj, 2015; Zheng *et al.*, 2014; Taleb and Ksentini, 2015; Rajamohamed and Rajamani, 2015; Nguyen *et al.*, 2013; Liu *et al.*, 2011). Both AODV and AOMDV are implemented and validated within the ns-2 code. The simulation model uses two main components to represent nodes mobility and data traffic, which are known as topology scenario and traffic scenario. The topology scenario describes the distribution of nodes over the simulation area and their movement during the simulation time, while the traffic scenario generates the data traffic between nodes. The topology scenarios were generated with the assistance of Bonnmotion tool (Aschenbruck *et al.*, 2010), to create VANET scenarios with group mobility. The scenarios are characterized by the following: Mobility model, number of nodes, average node speed, simulation area and simulation time. The nodes movement followed the RPGM mobility model described in Section 4. The traffic scenario, on the other hand, is characterized by the following: Number of data flows, type of data flow and traffic rate. In all simulated scenarios, nodes use the wireless standard IEEE 802.11p (Gerla and Kleinrock, 2011).

### Simulation Parameters

The performance analysis is conducted by simulating a VANET of 200 nodes moving over an area of size 2000×2000 m, for a period of 900 sec. These settings represent VANET scenarios in real life of moving vehicles moving in an open terrain like in a safari trip, a Sahara trip, or search and rescue operations, where communication between vehicles can be necessary while the communication infrastructure might not be available. Although the simulation settings in terms of number of nodes and simulation time could be higher, however, this is to keep the simulation processing time manageable. The protocols have been challenged under identical environmental conditions with identical loads using Constant Bit Rate (CBR) data flows in order to enable direct and fair comparison between the protocols.

Table 1. The parameters used in the simulation experiments

Parameter	Values
Number of nodes	200
MAC layer	IEEE 802.11 p
Simulation area	2000×2000 m
Simulation time	900 s
Mobility model	RPGM
Group size	5 nodes
Distance deviation	50 m
Average speed	10 m/s
Pause time	0 s
Traffic type	CBR
Packet size	512 bytes
Packet rate	8 packets/s
Number of flows	10, 20, 30, 40, 50, 60, 70, 80, 90

The traffic rate has been set to 8 packets/s. It is worth to note that simulations for a traffic rate of 16 packets/s have shown that the majority of packets were dropped due to congestion for both protocols, while for lower traffic rates it were found not ideal to measure the performance merits of the examined protocols. The packet size has been set to 512 bytes, for each traffic scenario. The number of flows has been varied between 10 to 90 flows. The number of flows was increased until the network became saturated with traffic.

Mobile nodes move according to the RPGM mobility model described in section 4. Nodes are divided into groups and build their movements based on the group leader movement. The number of nodes per group is set to 5 nodes. Each group leader selects a random destination and moves towards it, while the other members follow it with a maximum distance deviation of 50 m. The leader nodes speed is set randomly with a mean speed of 10 m/s. When the leader node reaches the desired destination, it pauses for the defined pause time. This movement behaviour continues all over the duration of the simulation time. To allow continuous movement of nodes, the pause time has been set to 0 sec, in all of the simulated scenarios. The nodes average moving speed has been set to 10 m/s representing regular safe vehicle speed limit. Each point in the simulation results, represents an average of 30 runs of randomly generated topologies, which were enough to calculate a 95% confidence interval with small relative errors. Simulation parameters are illustrated in Table 1.

## Results and Discussion

The performance of AODV and AOMDV is measured through five performance metrics: Throughput, end-to-end delay, normalised end-to-end delay, normalised average load and normalised routing overhead. The throughput is defined as the amount of successfully delivered data packets to the destination during the simulated time. This measure shows the efficiency of the protocol as it demonstrates the amount

of data the protocol is able to deliver in the network. The end-to-end delay is defined as the average amount of time data packets take to be delivered to their destinations, it includes all the possible delays that can occur to the packet from its generation to its delivery. The normalised end-to-end delay is calculated by dividing the end-to-end delay by the number of received packets. This measure provides better understanding of the achieved end-to-end delay as it considers the amount of received data. The normalised average load is calculated by dividing the average load of the forwarded data by the delivery ratio. The average load  $\mu$  is calculated as illustrated in Equation 3, where  $l_i$  represents the load of node  $i$ ; which is calculated by accumulating the lengths of data packets forwarded by the node and  $M$  represents the total number of forwarding nodes. The normalised average load  $NL$  is defined according to Equation 4, where  $d$  represents the delivery ratio. This metric measures the ability of the protocol in distributing the data traffic loads while being able to deliver the data to its final destination. The normalised routing overhead is calculated by dividing the total number of routing packets; which includes all control packets used to establish and maintain routes during the simulated time, by the number of received data packets. This measure captures the overhead generated by the protocol while considering its ability to deliver data packets:

$$\mu = \frac{\sum_i^M l_i}{M} \quad (3)$$

$$NL = \frac{\mu}{d} \quad (4)$$

In the following figures, the  $x$ -axis represents the variations in number of flows, while the  $y$ -axis represents the results of the performance metric of interest.

### Throughput

Figure 1 shows the data throughput for AODV and AOMDV. The two protocols have been challenged to the same simulation scenarios. As the figure illustrates, AODV and AOMDV show close performance when the number of flows varied between 10 and 30 flows. These scenarios represent traffic between group leaders. However, as we increase the number of flows, AOMDV clearly outperforms AODV with an amount that reaches triple the throughput achieved by AODV. Which means that AODV is not suitable for applications that involve large number of interactive users with heavy traffic requirements. Although AOMDV outperforms AODV in all scenarios with

heavy traffic, it is worth noting that both protocols have low delivery ratios after increasing the traffic beyond the 70 flows where AOMDV manages to deliver around 40% of the data whereas AODV delivers around 22% only. Naturally, as depicted in the figure these ratios decrease as the number of flows increases.

### End-to-End Delay and Normalised End-to-End Delay

Figure 2 shows the end-to-end delay of the two protocols. As the figure illustrates, for relatively low traffic with number of flows of 10 to 30 flows, AOMDV and AODV exhibit close performance. However, for heavier traffic, as we increase the number of flows, AOMDV clearly outperforms AODV not only in terms of end-to-end delay but also in the achieved throughput, this continues until the number of flows become 70 flows and above. Increasing the number of flows to 70 and beyond has affected both protocols. AODV demonstrates relatively steady behaviour of 400-600 ms. The end-to-end delay achieved by AOMDV increases sharply when the traffic goes beyond the 70 flows. However, we should bear in mind the higher delivery ratios that AOMDV achieved in most of the simulated scenarios. This can be depicted clearly when considering the normalised end-to-end delay in Fig. 3, which also demonstrates that AOMDV outperforms AODV in the majority of the scenarios even after increasing the traffic to 70 and beyond.

### Normalised Average Load

Figure 4 shows the normalised average load for AODV and AOMDV. This measure is intended to capture the ability of distributing the data traffic over the nodes in the network while delivering the data traffic correctly to its destination. As the figure illustrates, AOMDV outperforms AODV, although AOMDV achieves higher throughput in most of the simulated scenarios. The main reason behind this merit is that AOMDV distributes the load by nature through the alternative paths it generates. As the figure illustrates, AOMDV outperforms AODV with an average difference of 60%.

### Normalised Routing Overhead

Figure 5 shows the normalised routing overhead for AODV and AOMDV. As the figure illustrates, for the relatively low number of flows both protocols exhibit close performance. However as soon as the number of flows increases, AOMDV outperforms AODV with a difference reaches 99% lower than that of AODV. This behaviour continues to grow as we increase the traffic where AOMDV clearly overtake the situation. AODV generates 39 times the overhead generated by AOMDV, which means that AODV cannot cope with heavy traffic loads.

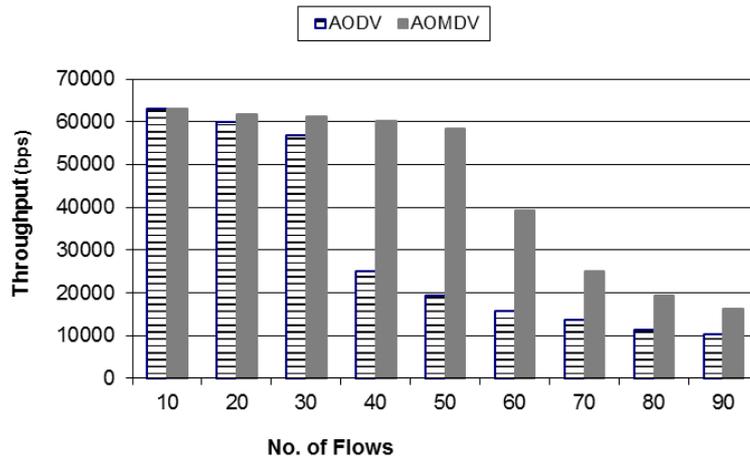


Fig. 1. Throughput of AODV and AOMDV

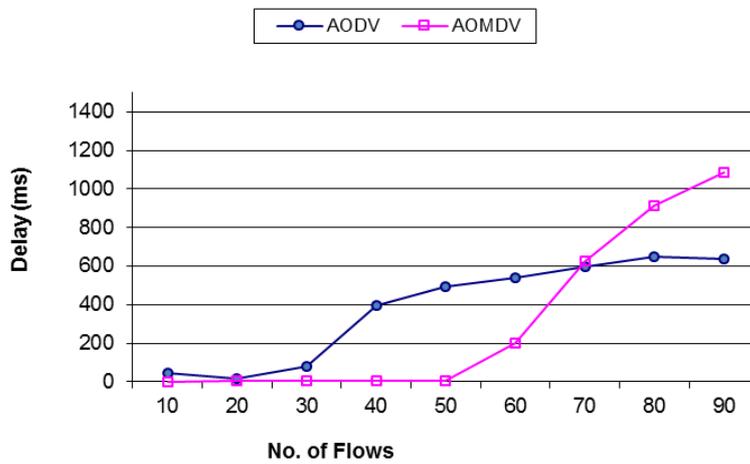


Fig. 2. End-to-end delay of AODV and AOMDV

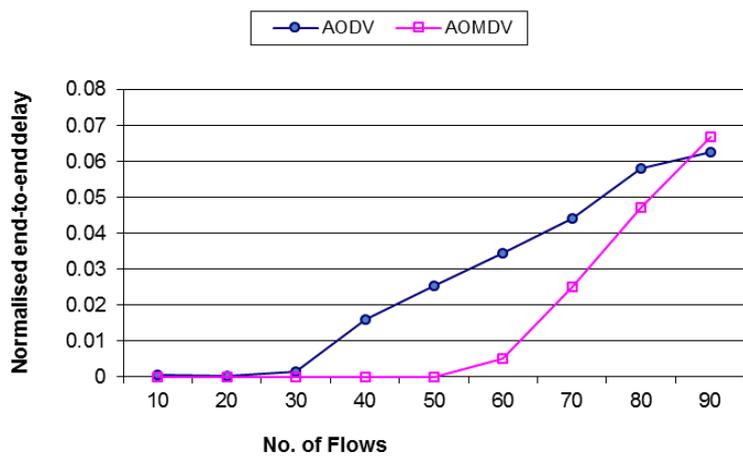


Fig. 3. Normalised end-to-end delay of AODV and AOMDV

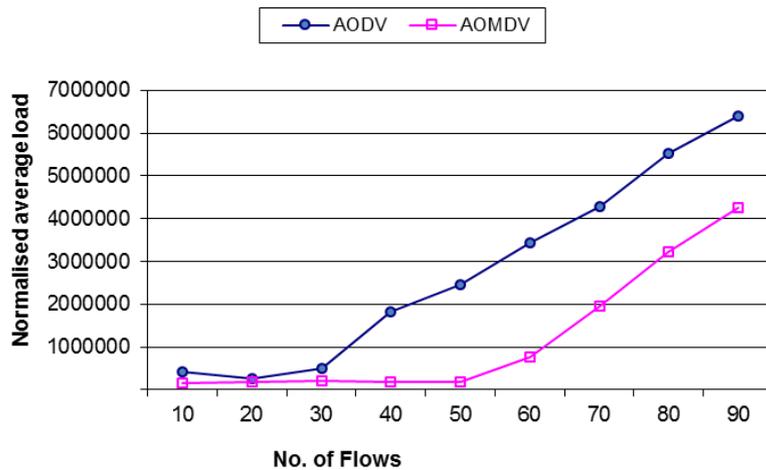


Fig. 4. Normalised average load of AODV and AOMDV

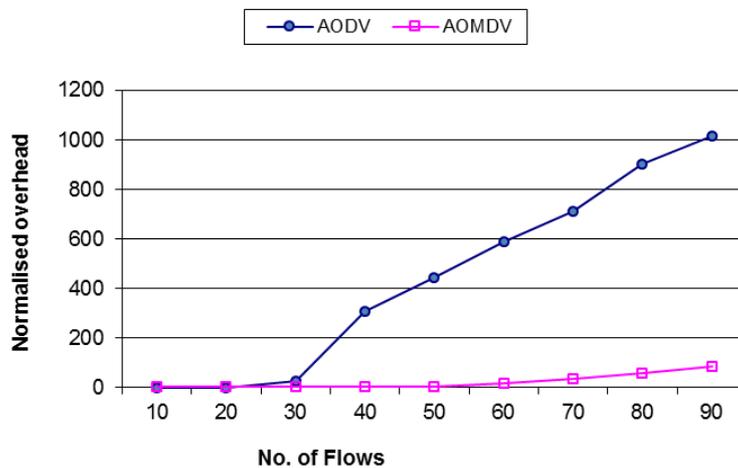


Fig. 5. Normalised routing overhead load of AODV and AOMDV

## Conclusion

Group communication can play important role in many VANET applications. It is of great importance to understand the impact of group mobility model on the performance of routing protocols as this can affect the overall performance of the network. The group concept is applied at various levels in the network protocol stack. In this study, extensive simulation experiments for both AODV and AOMDV has been conducted under the RPGM mobility model to study the impact of group mobility on their performance. The simulation results have shown that both protocols have comparable performance merits when the number of participating nodes is low, as in the case of group leaders' communication. Increasing the number of participating nodes has demonstrated a performance advantage for AOMDV, in the majority of performance metrics. AOMDV have shown to be a clear winner in terms of throughput, normalised

average load and normalised routing overhead. Hence, it has the ability to deliver data, distribute the traffic load and save energy. Which makes AOMDV more applicable for applications that require high throughput like audio or video streaming. It can also be suitable for live applications however when the number of participating nodes represent no more than half of the nodes in the network according to the conducted simulations, as its performance degrades after that. AODV on the other hand can be suitable for scenarios with low number of participating nodes, however we should bear in mind that it has a lower ability to distribute the traffic load and save energy.

## Acknowledgment

Part of this research was conducted during my staff exchange between Princess Sumaya University for Technology and Technical University of Berlin under the Avempace III project - Erasmus Mondus Programme.

## Ethics

This article is original and contains unpublished material. There are no ethical issues associated with publishing it.

## References

- Ahmed, E.F., R.A. Abouhogail and A. Yahya, 2014. Performance evaluation of blackhole attack on VANET's routing protocols. *Int. J. Software Eng. Applic.*, 8: 39-54.
- Al-Qassas, R.S., 2015. On the trade-off between multipath and single path routing in VANETs. *J. Next Generat. Inform. Technol.*, 6: 14-23.
- Al-Sultan, S., M.M. Al-Doori, A.H. Al-Bayatti and H. Zedan, 2014. A comprehensive survey on vehicular Ad Hoc network. *J. Netw. Comput. Applic.*, 37: 380-392.  
DOI: 10.1016/j.jnca.2013.02.036
- Amjad, K., 2011. Performance analysis of DSR protocol under the influence of RPGM model in mobile ad-hoc networks. *Proceedings of the 31<sup>st</sup> International Conference on Distributed Computing Systems Workshops*, Jun. 20-24, IEEE Xplore Press, Minneapolis, MN., pp: 100-104.  
DOI: 10.1109/ICDCSW.2011.57
- Anggoro, R., T. Kitasuka, R. Nakamura and M. Aritsugi, 2012. Performance evaluation of AODV and AOMDV with probabilistic relay in VANET environments. *Proceedings of the 3rd International Conference on Networking and Computing*, Dec. 5-7, IEEE Xplore Press, Okinawa, pp: 259-263.  
DOI: 10.1109/ICNC.2012.47
- Arulkumar, N. and E.G.D.P. Raj, 2015. CBAODV: An enhanced reactive routing algorithm to reduce connection breakage in VANET. *Proceedings of the International Conference on Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*, (AES' 15), Springer, pp: 533-539.  
DOI: 10.1007/978-81-322-2135-7\_57
- Aschenbruck, N., R. Ernst, E. Gerhards-Padilla and M. Schwamborn, 2010. BonnMotion: A mobility scenario generation and analysis tool. *Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniques*, Mar. 16-18, ICST, Malaga, Spain, pp: 1-10.  
DOI: 10.4108/ICST.SIMUTOOLS2010.8684
- Dhilipkumar, V., D. Kandar and C.K. Sarkar, 2013. Enhancement of inter-vehicular communication to optimize the performance of 3G/4G-VANET. *Proceedings of the International Conference on Optical Imaging Sensor and Security*, Jul. 2-3, IEEE Xplore Press, Coimbatore, pp: 1-5.  
DOI: 10.1109/ICOISS.2013.6678425
- Engoulou, R.G., M. Bellaïche, S. Pierre and A. Quintero, 2014. VANET security surveys. *Comput. Commun.*, 44: 1-13. DOI: 10.1016/j.comcom.2014.02.020
- Gerla, M. and L. Kleinrock, 2011. Vehicular networks and the future of the mobile internet. *Comput. Netw.*, 55: 457-469.  
DOI: 10.1016/j.comnet.2010.10.015
- Grover, J., M.S. Gaur, V. Laxmi and R.K. Tiwari, 2012. Detection of incorrect position information using speed and time span verification in VANET. *Proceedings of the 5th International Conference on Security of Information and Networks*, Oct. 22-26, ACM, Jaipur, India, pp: 53-59.  
DOI: 10.1145/2388576.2388583
- Hager, M., L. Wernecke, C. Schneider and J. Seitz, 2015. Vehicular ad hoc networks: Multi-hop information dissemination in an urban scenario. *Proceedings of the 38th International Conference on Telecommunications and Signal Processing*, Jul. 9-11, IEEE Xplore Press, Prague, pp: 65-70.  
DOI: 10.1109/TSP.2015.7296225
- Jayakumar, G. and G. Ganapathi, 2008. Reference point group mobility and random waypoint models in performance evaluation of MANET routing protocols. *J. Comput. Syst. Netw. Commun.*, 2008: 860364-860376. DOI: 10.1155/2008/860364
- Jiajia, L., N. Kato, M. Jianfeng and T. Sakano, 2015. Throughput and delay tradeoffs for mobile ad hoc networks with reference point group mobility. *IEEE Trans. Wireless Commun.*, 14: 1266-1279.  
DOI: 10.1109/TWC.2014.2365553
- Kabir, T., N. Nurain and M.H. Kabir, 2015. Pro-AODV (Proactive AODV): Simple modifications to AODV for proactively minimizing congestion in VANETs. *Proceedings of the International Conference on Networking Systems and Security*, Jan. 5-7, IEEE Xplore Press, Dhaka, pp: 1-6.  
DOI: 10.1109/NSysS.2015.7043521
- Lin, G., G. Noubir and R. Rajaraman, 2004. Mobility models for ad hoc network simulation. *Proceedings of the 23th Annual Joint Conference of the IEEE Computer and Communications Societies*, Mar. 7-11, IEEE Xplore Press.  
DOI: 10.1109/INFCOM.2004.1354517
- Liu, Y., Y. Wang, S. Chen, X. Li and Z. Rao, 2011. A hybrid MAC mechanism for multiple load intelligent vehicle transportation network. *Int. J. Smart Sens. Intell. Syst.*, 4: 662-674.
- Marina, M.K. and S.R. Das, 2001. On-demand multipath distance vector routing in ad hoc networks. *Proceedings of the International Conference on Network Protocols*, Nov. 11-14, IEEE Xplore Press, pp: 14-23. DOI: 10.1109/ICNP.2001.992756

- Mejri, M.N., J. Ben-Othman and M. Hamdi, 2014. Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Commun.*, 1: 53-66. DOI: 10.1016/j.vehcom.2014.05.001
- Moravejosharieh, A., H. Modares, R. Salleh and E. Mostajeran, 2013. Performance analysis of AODV, AOMDV, DSR, DSDV routing protocols in vehicular ad hoc network. *Res. J. Recent Sci.*, 2: 66-73.
- Nagaraj, M.U. and M.P.P. Dhamal, 2012. Performance comparison of AODV, AOMDV, OLSR, DSR and GSR routing protocols in VANET. *Proceedings of the International Conference on Advances in Computer, Electronics and Electrical Engineering, (EEE' 12)*, Universal Association of Computer and Electronics Engineers, pp: 394-398. DOI: 10.3850/978-981-07-1847-3P0898
- Nguyen, T.V., F. Baccelli, K. Zhu, S. Subramanian and X. Wu, 2013. A performance analysis of CSMA based broadcast protocol in VANETs. *Proceedings of the IEEE INFOCOM, Apr. 14-19*, IEEE Xplore Press, Turin, pp: 2805-2813. DOI: 10.1109/INFOCOM.2013.6567090
- Perkins, C.E., E.M. Belding-Royer and S.R. Das, 2003. Ad hoc On-demand Distance Vector (AODV) routing, RFC 3561. Internet Engineering Task Force.
- Perlman, R., 1992. *Interconnections: Bridges and Routers*. 1st Edn., Addison-Wesley, Reading ISBN-10: 0201563320, pp: 389.
- Rajamohamed, R. and V. Rajamani, 2015. TLS: Improving security for mobility based MANET using three level security mechanism. *Int. J. Applied Eng. Res.*, 10: 16585-16594.
- Ravi, K. and K. Praveen, 2014. AODV routing in VANET for message authentication using ECDSA. *Proceedings of the International Conference on Communication and Signal Processing, Apr. 3-5*, IEEE Xplore Press, Melmaruvathur, pp: 1389-1393. DOI: 10.1109/ICCSP.2014.6950077
- Sakthi Ganesh, M. and P. Venkata Krishna, 2013. Improving frequent link failure detection in VANET. *Int. J. Eng. Technol.*, 5: 1882-1886.
- Sampigethaya, K., M. Li, L. Huang and R. Poovendran, 2007. AMOEBA: Robust location privacy scheme for VANET. *IEEE J. Selected Areas Commun.*, 25: 1569-1589. DOI: 10.1109/JSAC.2007.071007
- Simaremare, H., A. Syarif, A. Abouaissa, R.F. Sari and P. Lorenz, 2013. Performance comparison of modified AODV in reference point group mobility and random waypoint mobility models. *Proceedings of the IEEE International Conference on Communications, Jun. 9-11*, IEEE Xplore Press, Budapest, pp: 3542-3546. DOI: 10.1109/ICC.2013.6655100
- Taleb, T. and A. Ksentini, 2015. VECOS: A vehicular connection steering protocol. *IEEE Trans. Vehicular Technol.*, 64: 1171-1187. DOI: 10.1109/TVT.2014.2327241
- Thenmozhi, R. and S. Govindarajan, 2016. Safety related services using smart vehicle connections. *Int. J. Applied Eng. Res.*, 11: 2384-2387.
- Verma, S., P. Nayak and R. Agarwal, 2013. Performance analysis of energy aware routing schemes under various mobility models. *Proceedings of the International Conference on Communications and Signal Processing, Apr. 3-5*, IEEE Xplore Press, Melmaruvathur, pp: 475-478. DOI: 10.1109/iccsp.2013.6577099
- Vidhale, B. and S.S. Dorle, 2011. Performance analysis of routing protocols in realistic environment for vehicular ad hoc networks. *Proceedings of the International Conference on Systems Engineering, Aug. 16-18*, IEEE Xplore Press, Las Vegas, NV., pp: 267-272. DOI: 10.1109/ICSEng.2011.55
- Weerasinghe, H., H. Fu and S. Leng, 2010. Anonymous service access for vehicular ad hoc networks. *Proceedings of the Sixth International Conference on Information Assurance and Security, Aug. 23-25*, IEEE Xplore Press, Atlanta, GA., pp: 173-178. DOI: 10.1109/ISIAS.2010.5604052
- Whaiduzzaman, M., M. Sookhak, A. Gani and R. Buyya, 2014. A survey on vehicular cloud computing. *J. Netw. Comput. Applic.*, 40: 325-344. DOI: 10.1016/j.jnca.2013.08.004
- Xi, W., L. Si, Z. Huibiao and Z. Yongxin, 2014. Reasoning about group-based mobility in MANETs. *Proceedings of the IEEE 20th Pacific Rim International Symposium on Dependable Computing, Nov. 18-21*, IEEE Xplore Press, Singapore, pp: 244-253. DOI: 10.1109/PRDC.2014.39
- Yufeng, C., X. Zhengtao, J. Wei and J. Weirong, 2009. A cross-layer AOMDV routing protocol for V2V communication in urban VANET. *Proceedings of the International Conference on Mobile Ad-hoc and Sensor Networks, Dec. 14-16*, IEEE Xplore Press, Fujian, pp: 353-359. DOI: 10.1109/MSN.2009.30
- Zheng, J., Y. Wu, Z. Xu and X. Lin, 2014. A reliable routing protocol based on QoS for VANET. *Proceedings of the International Conference on Advanced Infocomm Technology, Nov. 14-16*, IEEE Xplore Press, Fuzhou, pp: 21-28. DOI: 10.1109/ICAIT.2014.7019524