

A Trust-based Stable Routing Protocol in Vehicular ad-hoc Networks

Junxia Ma* and Chen Yang

Zhengzhou University of Light Industry
jxma@zzuli.edu.cn; chenyang@zzuli.edu.cn

Abstract

One of the greatest challenges in vehicular ad-hoc networks (VANET) is to establish stable routing. Due to dynamic network, keeping stable routing is a difficult problem. Therefore, trust-based stable routing (TBSR) protocol is proposed in this paper. The node is chosen to be next-hop node until it reaches to trust threshold. To evaluate the node trust, we introduce the node's role trust, interaction printer trust, and recommendation trust. Moreover, the Analytic Hierarchy algorithm is used to coalesce various recommendation opinions from neighbor nodes. The simulation results show that the proposed approach outperforms GPSR (greedy perimeter stateless routing) and OLSR (optimized link-state routing) in terms of throughput, average delay.

Keywords: VANET, routing protocol, trust, Analytic Hierarchy

1. Introduction

With the advance and wide deployment of wireless communication technologies, vehicle manufactures and research academia are heavily engaged in the blueprint of future VANET. Vehicles in a VANET communicate with each other by sharing road condition and safety information, to enhance passenger and road safety and to effectively route traffic through dense urban areas[1]. VANET is self-configuring network which consists of vehicles, elements of road side infrastructure, sensors and pedestrian personal[2]. It can be easily deployed without relying on expensive network infrastructure. However, the limited coverage of WiFi and the high mobility of the nodes generate frequent topology changes and network fragmentations. These characters make communication between vehicles and preexisting fixed infrastructure unstable. So the effective application of VANET revolves around a lot of key elements such as message routing. Without an effective routing protocol, the application of VANET will be limited [3].

Traditional routing protocols for MANET (mobile ad hoc networks) demonstrated that their performance is poor in VANET [4-5]. Such as optimized link-state routing (OLSR) [6], dynamic source routing [7], ad-hoc on demand distance vector routing (AODV) [8], and greedy perimeter stateless routing (GPSR) [9]. These routing is instability due to particular environments. Indeed, since that there are in the presence of node with high mobility in VANET, the traditional node-centric view of the routes is frequently broken, which results in dropping many packets and makes delivery ratios low and transmission delays high[10].

Thus, it is acceptable to use trust-based routing as a stable solution, in which a trust-based scheme is used to protect the routing protocol. Every node in VANET independently executes a trust model to evaluate the trust it has on other nodes. This evaluated trust value is used during routing decisions. Trust-based routing protocols attempt to establish most trusted routes, which make the routing more stable[11].

The remainder of the paper is organized as follows. The evaluating node-trust value is analyzed in section II. Numerical results and comparisons with GPSR and OLSR were presented in section III. Finally, concluding remarks are drawn in section IV.

2. Relate Work

In VANET, vehicular network security is greatly important, which usually refer to trust relations in a public key infrastructure. Security mechanism mainly provides identification of entities but not trust in the sense of this paper. Raya et.al[5]give a wally overview on security aspects and mechanisms in vehicular networks. For data verification, they first considered reputation ,but then developed their own data-centric trust model [7].While their model focuses only on the data , the proposed model focuses only on the sender. So,both models complete each other. Reference [6] also verifies the data, this time based on a model of the network.

Vehicular ad hoc networks are similar to wireless sensor networks. In both networks mainly sensory data is exchanged. The framework of Zhang[9] served as a starting point for our work. In contrast to their scenarios, a car receives less reports about the same subject, but it can get to specific places (if the driver does so) to verify the received information itself.

In the area of electronic marketplaces, reputation systems are well known (e.g. eBay's feedback system[10], the beta reputation system [11], or even Google's PageRank [12]). Here, the trust comes from human beings. The reputation system then combines these statements to build a global view on an entity – the reputation. To get this global view, reputation systems work on the network level. In contrast, the trust directly comes from artificial agents in purely electronic market places of multi-agent systems. Sabater and Sierra [13] give a good overview of the trust and reputation models in this area.

In addition, routing protocol play an important role on VANET application. However, Traditional wireless ad-hoc network routing protocols, such as Ad hoc On-Demand Distance Vector (AODV), are not suitable for VANETs due to end to end path selection criteria. To deal with the rapidly changing network topology, routing techniques based on location information are considered more suitable. Greedy Perimeter Stateless Routing (GPSR) selects the vehicle that is closest to the destination among the neighboring vehicles. When local maximum occurs, the algorithm recovers by routing around the perimeter of the region. Data is then forwarded opportunistically without consideration of road topology and network connection status. The Geographical Source Routing (GSR) protocol uses position information and considers the road topology as a connected graph with edges and vertices[12]. It also forwards data opportunistically.

Vehicle-Assisted Data Delivery (VADD) is a vehicular routing protocol aimed at improving routing in disconnected vehicular networks in urban scenarios [13]. In a disconnected scenario it uses carry and-forward approach until a relay is found. Geographical Opportunistic (GeoOpps) is a delay tolerant network routing algorithm that exploits the availability of information from the NS in order to opportunistically route a data packet to a certain geographical location [14].

Numerous PBR protocols are proposed or adopted for VANETs. The majority of PBR protocol have not considered a realistic Location Service in their evaluation and assumed the availability of destination location. Destination location can be obtained via the pure ad hoc network or another network such as cellular or sensor networks which can affect protocols performance and communication cost. In the route selection process, protocols deploy different methods such as pure geographic, anchor-based [15, 17, 19], static information such as map [18] and bus routes [19], statistics information and real-time information [20].

The vast majority of protocols give priority to dense roads for better network connectivity which causes data traffic congestions. Vehicles can also act as communication obstacles which increase the number of packet forwarders as well as packet retransmissions. Moreover, it is common in city scenarios to have vehicles clustered around traffic lights, while the VANET is intermitted at the middle of the roads. Thus, selecting dense areas in the routing process is not an accurate criterion.

3. Node-trust Value

Trust in entities is based on the fact that the trusted entity will not act maliciously. Trust has the following characteristics:

it is subjective. Different nodes may have different perceptions of the same node's trustworthiness;

it is asymmetric, Two nodes don't need to have similar trust in each other;

it is time dependent. It grows and decays over period of time and it is based on previous similar experiences with the same party.

In VANET, a trust relationship that formed from direct interactions can be characterized as direct trust. A trust relationship or a potential trust relationship built from recommendations by a trusted node or chain of trusted nodes, which create a trust path, is called indirect trust. Moreover, the use of recommendations can speed up the convergence of the trust evaluating process.

In this paper, Trust value shows the degree that one node deal with the data from another node, which is a relationship one another. In order to obtain accurate node-trust value, an evaluating node should collect all relevant information about an evaluated node, including the node's role, interaction records, opinions from other nodes. In our scheme, node-trust value consist of three portion ,node's role trust value, interaction printer trust value and recommendation trust value, respectively. We use the AHP to compute the weights of three portion.

3.1. Node's Role Trust

Motivated by the approach of [11], we exploit three predefined roles assigned to all nodes in the system. The three roles are listed in decreasing order that from the highest role to the lowest one. Each role level is corresponding to a trust value $T_r \in (0,1)$, where lower level roles have smaller T_r values.

1) law role: there are a minority of vehicles, such as police cars and traffic controllers, law enforcement, state or municipal police in VANET. There vehicles possess high credibility in the society due to those special status that regulating people's behavior. Without loss of generality, assume that there vehicle have the highest trust value.

2) public role: there are some public services car, such as ambulance, school bus, road maintenance, public transits. There vehicles provided public service, discharged public responsibilities, crafted good public image. Therefore, assume that there vehicle have higher trust value.

3) general role: the remainder vehicles have general identity. These vehicles are considered having general role. Therefore ,trust value of them is below law role and public role.

All vehicles should possess certificates containing vehicle's role and the certificates should be issued by a central authority(CA).In our scheme, we use the public key certificates in an asymmetric crypto system to guarantee that a certain vehicle can acquire another vehicle real role. Every vehicle possess a public key certificate containing the vehicle's ID, role and public key. The certificate is signed by CA. Each vehicle is able to verify the CA's signature by using his public key.

3.2. Interaction Printer Trust

Interaction printer trust is trust relationship established by direct interaction . In our scheme, the direct interaction occurs between a vehicle and its physical neighbour. Interaction printer trust evaluation is based on two vehicle historical interaction information. Assuming that vehicle v_i and v_j , v_i is the evaluating vehicle; v_j is the evaluated vehicle by v_i . v_i make a interaction printer trust evaluation on v_j , which is based on the direct interaction on the time t . The trust evaluation is denoted by $f(t, i, j)$, and $f(t, i, j) \in (0,1)$.

Every evaluation results are stored in the evaluating vehicle memory. In order to compute an accurate interaction printer trust value, the interaction time freshness is considered, which is time lag between last evaluation and now. Generally, the greater the time lag, the faster the time freshness decline is. We use a coefficient σ to represents the decline factor. Finally, vehicle v_i computes a direct interaction trust value for vehicle v_j according to their history interaction evaluation by the equation (1)

$$f(t, i, j) = \frac{1}{N} \sum_{m=1}^N \sigma^{t-t_m} f(t_m, i, j) \quad (1)$$

Where N is the number of interactions by the end of time t . σ^{t-t_m} is the weighted of interaction evaluation $f(t_m, i, j)$. The coefficient σ can be adjusted according to different environment. $\sigma \in (0,1)$. In addition, if vehicle v_i has no direct interaction with vehicle v_j , $f(t, i, j) = 0$.

3.3. Recommendation Trust Value

We consider the evaluated vehicle's physical neighbour vehicle's opinion in order to alleviate the influence from evaluating vehicle's subjective manners, besides, a situation always exists: evaluating vehicle has no direct interaction with evaluated vehicle, but recommending vehicles (evaluated vehicle's physical neighbour vehicles) have direct interaction with evaluated vehicle. Therefore, it is very necessary to take recommending vehicles' opinion into account. In addition, adopting recommending vehicles' opinion, evaluated vehicle should take account of its role. The weight value of recommending vehicles' opinion change with role. For example, if a recommending vehicle is police car, his recommending opinion emphatically considered and carries a big weight. The opinion of recommending vehicle v_k about vehicle v_j is denoted by R_T_{kj} . We can calculate

$$R_T_{kj} = T_r^k * f(t, k, j) \quad (2)$$

Where, T_r^k denotes the vehicle v_k role trust value.

Evaluating vehicle v_i collect all recommendation trust value from recommending vehicles and final recommendation trust value R_T_j for v_j is computed by equation (3)

$$R_T_j = \frac{1}{N_r} \sum_{k=1}^{N_r} R_T_{kj} \quad (3)$$

Where, N_r is the number of recommending vehicles about vehicle v_j .

On the basis of the mentioned analysis, the node-trust value T_node_{ij} , which is composed of node's role trust T_r^j , interaction printer trust $f(t, i, j)$ and recommendation trust value R_T_j .

$$T_node_{ij} = \alpha T_r^j + \beta f(t, i, j) + \varepsilon R_T_j \quad (4)$$

Where $\alpha, \beta, \varepsilon$ are coefficients and $\alpha + \beta + \varepsilon = 1$. The values of $\alpha, \beta, \varepsilon$ are decided by the influencing on the evaluation of trust value in different application environment. However, it is different to determine these precise weights.

3.4. Weights

Motivated by the approach of [7], we use AHP theory to determine the weights. The key step is to establish a judgment matrix by nine-point position scaling method. The credibility measuring are shown in Table 1.

Table 1. Standard Preference

Numerical value	Preference level
1	Equal importance
3	moderate importance of one over another
5	essential or strong importance
7	very strong importance
9	extreme importance
2,4,6,8	Intermediate values between the above two adjacent judgments

Reciprocals: if activity i has value a_i when it compared with activity j , then j has the reciprocal value when compared with i .

As Table 1 shows, we need to compare the importance of each related factor (node's role trust T_r^j , interaction printer trust $f(t,i,j)$, recommendation trust value R_T_j). It is a neuralgic issue.

For a different environment, the role that each factor impersonate is different. Therefore, no one is more important than another. Only in a given environment, the importance of each factor is determined. In fact, the values themselves ($T_r^j, f(t,i,j), R_T_j$) calculated by above method reflect the environment information. For example, R_T_j is larger, which mean that there are more vehicles in network. Consequently, the judgment matrix is established by the values themselves. The principle that the value is big and it is more important than another. Assuming that the judgment matrix is:

$$A = \begin{matrix} & \begin{matrix} T_r^j & f(t,i,j) & R_T_j \end{matrix} \\ \begin{matrix} T_r^j \\ f(t,i,j) \\ R_T_j \end{matrix} & \begin{pmatrix} 1 & a & b \\ 1/a & 1 & c \\ 1/b & 1/c & 1 \end{pmatrix} \end{matrix} \quad (5)$$

The issue then is to identify the value of a, b, c . According to the above principle, using the concept of standardization, let

$$a = \begin{cases} \lfloor T_r^j / f(t,i,j) \rfloor & \text{if } |T_r^j| > |f(t,i,j)| \\ 1 / \lfloor f(t,i,j) / T_r^j \rfloor & \text{other} \end{cases} \quad (6)$$

Where $\lfloor \bullet \rfloor$ denote the math floor. For example, $\lfloor 3.5 \rfloor = 3$. In the same way, b, c be computed.

For example, $T_r^2 = 0.9$; $f(3,1,2) = 0.2$; $R_T_2 = 0.3$ then judgment matrix is $A = \begin{pmatrix} 1 & 4 & 3 \\ 1/4 & 1 & 1 \\ 1/3 & 1 & 1 \end{pmatrix}$.

Based on the equal (6), the judgment matrix is obtained and utilize the AHP theory to determine the weights. The algorithm is as follows.

Algorithm 1

-
- Step1: Each column vector of the judgment matrix A is normalized: $\tilde{a}_{ij} = a_{ij} / \sum_{i=1}^3 a_{ij}$
- Step2: \tilde{a}_{ij} is summed by row: $\tilde{a}_i = \sum_{j=1}^3 \tilde{a}_{ij}$
- Step3: \tilde{a}_i is normalized: $a_i = \tilde{a}_i / \sum_{i=1}^3 \tilde{a}_i$
- Step4: $a = (a_1, a_2, a_3)^T$ is the weight vector $(\alpha, \beta, \varepsilon)$
-

4. Description of TBSR Protocol

In TBSR, each node can obtain knowledge about neighbour nodes. TBSR protocol uses periodic HELLO messages for information sharing, it contains position direction, speed and trust value. The idea is to implement forwarding logic into forwarding node (which holds the packet) to select the next-hop vehicle as relay according to information acquired through trust value. If the next-hop node's trust value is more than threshold, the node relay the packet. In other words, the forwarding node will select the next-hop node that have high trust value.

Recovering from a disconnected link using node's current position and the destination of the packet is not sufficient. Therefore, trust value is vital when deciding the next hop node. Suppose a forwarding node needs to forward the packet to the next-hop node within the range and direction towards the destination region. Trust value of nodes can be used effectively to predict the optimal relay.

In addition, the operation of TBSR protocol can be assumed in two parts: 1) mobility knowledge acquisition and 2) packet sending process.

4.1. Mobility Knowledge Acquisitions

In TBSR protocol, each node sends position and vector information to its neighbour. Therefore each node in the network acquires sufficient information regarding the local topology and the neighbour of 1-hop neighbour for next hop selection. Periodic transmission of messages occupies the network sources, but it serves as trade-off between accurate relay prediction and network saturation in a self-organizing vehicular network. acquired mobility information serves as an input to the packet sending process for relay selection and forwarding.

4.2. Packet Sending Process

TBSR protocol is based on the assumption that every node in participating network has enough knowledge of its own and neighbour location and direction, speed and trust value. Subsequently, Figure 1 illustrates the full procedure of TBSR protocol. As shown as Figure 1, source node S transmits a packet to a destination node D . At first, it searches its neighbour area for destination information, if found, S transmits directly to D . If the destination node is not in the neighbour area, S select a best next-hop forwarding node according to trust value.

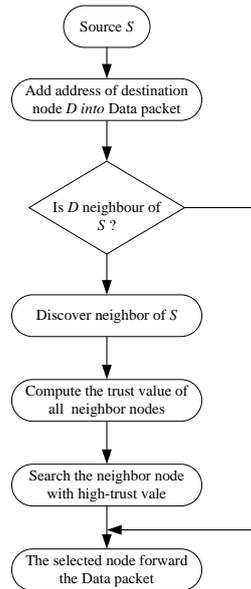


Figure 1. Flowchart of TBSR Protocol

5. Simulation and Performance Evaluation

In this section, in order to evaluate the effectiveness of our scheme, we design our simulation, which were done using ns 2.32, the underlying MAC protocol being 802.11.15. Nodes were randomly deployed in an area measuring 600m×15m. Transmission range of node is 300m. Numbers of nodes N varied from 10 to 140. Specifically, simulation parameter is shown as Table 2.

Table 2. Simulation Parameter

Parameter	Value
Simulation time	180s
Simulation area	600 m * 15 m
Number of nodes N	10-140
Speed	5-28m/s
Radio frequency	2.47GHz
Channel bandwidth	5.5Mbps
MAC protocols	IEEE 802.11b
Transmission range	300m

Our criteria for effectiveness are End-to-end delay, overhead and BER. The simulation model is as shown in Figure 2 below.

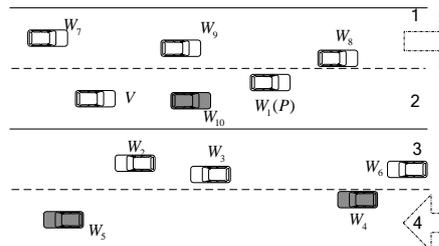


Figure 2. Simulation Model

In this section, we compare our proposal with respect to two routing protocols, GPSR[9], OLSR[6], respectively. The simulation results is as shown in Figure 3, 4 and 5 .

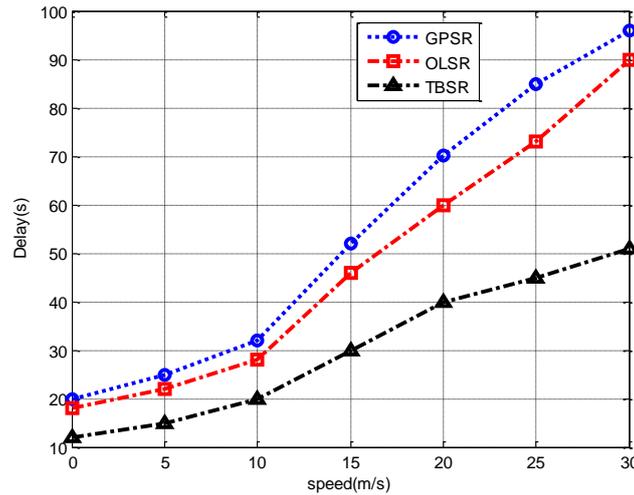


Figure 3. Impact of Variation of Speed on the End-to- end Delay (N=50)

Note that the results of Figure 3 are obtained assuming a multichannel environment. In such scenario, we can notice that the delay increase with the increase of speed from nodes. The reason is that, in case of low-speed network, the packet has to be relay by the node, whose moving speed is slower. The speed is more slower, the link is more stable. On the other hand, in high-speed networks, the communication link between node and node is more unstable. In this situation, the communication between nodes and nodes is difficult and the average number of break-link will increase. So the end-to-end delay will increase.

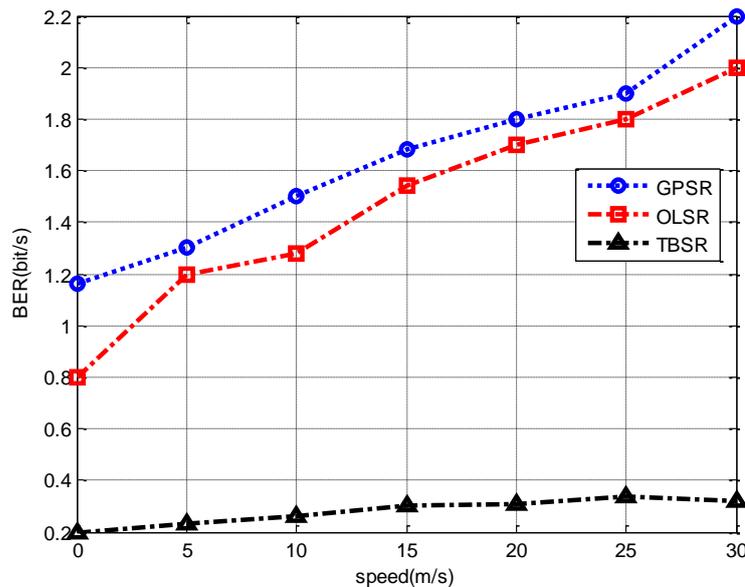


Figure 4. Impact of Variation of Speed on the BER (N=50)

Moreover, Figure 4 compares the BER for different speed. We can notice that the BER increases with the increase of speed. This is related to the fact that more high speed of nodes, the link is more unstable. So that, the BER increases. Compared with GPSR and

OLSR, the proposed algorithm has good performance and the BER is lower than GPSR and OLSR.

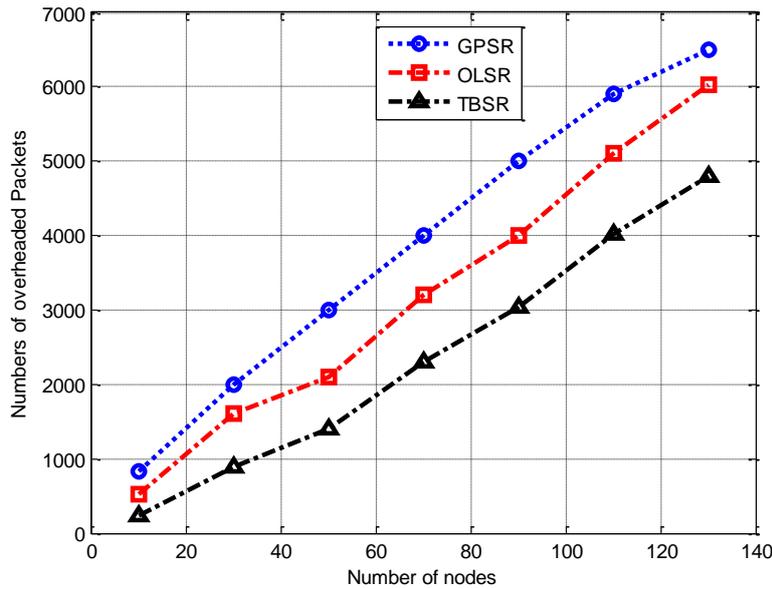


Figure 5. Impact of Variation of Number of Nodes on the Overhead Packet (speed=15m/s)

Figure 5 compares the overhead packet for different number of nodes with 15m/s. We can notice that the number of overhead packet increases with the increase of number of nodes. This is related to the fact that more much number of nodes, collision is more. So that, the overhead increases. Compared with GPSR and OLSR, the proposed TBSR has good performance and the overhead packet is lower than GPSR and OLSR.

6. Conclusion

In this paper, we have proposed a new approach for routing messages in city-based environments that takes advantage of trust management to improve the performance of routing in VANET. Our proposal scheme tends to satisfy performance metrics: end-to-end delay and BER. In our scheme, trust-based routing protocol is used. The trust a node has for a neighbour forms the basic building block of our trust model. The proposed trust evaluated technique, which is executed by every node in the network independently uses only local information thereby making it scalable. Moreover, unlike GPSR and OLSR, which based on location information that require a lot of space and time for buffering packets and computing the distance between nodes and nodes, our schemes does not require such an overhead. Simulation results show that the effectiveness of our approach.

Acknowledgements

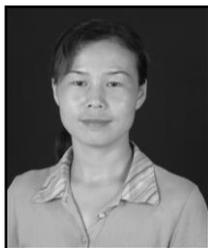
This work is supported by the Science & Technology Foundation of Education Department of Henan Province (No. 14A520062), the Science & Technology Foundation of Zhengzhou University of Light Industry (No. 2013XJJ018).

References

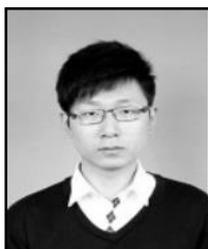
- [1] T. Jamal, G. N. Jose and A. Enrique, "Intelligent OLSR Routing Protocol Optimization for VANETS", *IEEE Transactions on Vehicular Technology*, vol.61, no. 4, (2012), pp. 1884-1895.
- [2] H. N. Saleet, R. Langar, K. Naik and A. Nayak, "Intersection-Based Geographical Routing Protocol for VANETs: A proposal and Analysis", *IEEE Transactions on Vehicular Technology*, vol. 60, no. 9, (2011),pp. 4560-4575.

- [3] C. Lochert, "A routing strategy for vehicular ad hoc network in the city environments", Proc. IEEE Intell. Veh. Symp., (2003).
- [4] V. Naumov and T. Gross, "Connectivity-Aware Routing (CAR) in vehicular adhoc networks", Proc. IEEE INFOCOM, (2007).
- [5] T. Clausen and P. Jacquet, "RFC 3626: The optimized link-state routing protocol", Internet Eng. Task Force Request For Comments, (2003).
- [6] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks", Mobile Comput., vol. 353, (1996), pp. 153– 181.
- [7] C. Perkins and E. Royer, " Ad-hoc on demand distance vector routing", Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl., (1999).
- [8] B. N. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks", Proc. ACM MOBICOM, (2000).
- [9] C. Lochert, B. Scheuermann, C. Wewetzer, A. Luebke and M. Mauve, "Data aggregation and roadside unit placement for a VANET traffic information system", Proc. ACM VANET, (2008).
- [10] N. March and R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks", IET Information security, vol. 6, no. 2, (2012), pp. 77-83.
- [11] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing in Mobile Computing Systems and Applications", Proceedings, WMCSA, Second IEEE Workshop, (2012).
- [12] C. Lochert, "A routing strategy for vehicular ad hoc networks in city environments", Intelligent Vehicles Symposium, Proceedings, IEEE, (2011).
- [13] J. Zhao and G. Cao, VADD: Vehicle-assisted data delivery in vehicular ad hoc networks, Vehicular Technology, IEEE Transactions, vol. 57, (2008), pp.1910-1922.
- [14] K. C. Lee, "Geo-opportunistic routing for vehicular networks", Communications Magazine, IEEE, vol.48, (2010), pp. 164-170.
- [15] C. Lochert, H. Hartenstein, J. Tian, H. Fussler, D. Hermann and M. Mauve, "A routing strategy for vehicular ad hoc networks in city environments", Proc. IEEE IVS, (2003).
- [16] M. Jerbi, S. Senouci, T. Rasheed and Y. G. Doudane, "Towards Efficient Geographic Routing in Urban Vehicular Networks, IEEE Trans. Veh. Technol., vol. 58, no. 9, (2009), pp. 5048-5059.
- [17] N. Alsharif, S. Cespedes and X. Shen, "iCAR: Intersection-based Connectivity Aware Routing in Vehicular Ad hoc Networks", Proc. IEEE ICC, (2013).
- [18] J. Tian, L. Han and K. Rothermel, "Spatially aware packet routing for mobile ad hoc inter-vehicle radio networks", Proc. IEEE ITS, (2011).
- [19] B. C. Seet, G. Liu, B. S. Lee, C. H. Foh and K. K. Lee, "A-STAR: A mobile ad hoc routing strategy for metropolis vehicular communications", Proc. Networking, (2014).
- [20] H. Saleet, R. Langar, K. Naik, R. Boutaba, A. Nayak and N. Goel, "Intersection-based geographical routing protocol for vanets: A proposal and analysis", Vehicular Technology, IEEE Transactions, vol. 60, no. 9, (2011), pp. 4560-4574.

Authors



Ma Junxia, female, was born in 1974, in Henan province. Now, she is lecturer, her main research area is artificial intelligence and knowledge engineering



Yang Chen, male, was born in 1987, in Henan province. Now, he is assistant, his main research area is machine learning and knowledge engineering.