A Similarity based Trust and Reputation Management Framework for VANETs

Nianhua Yang[1, 2]

*[1]Department of Computer Science & Engineering,
Shanghai Jiaotong University, Shanghai 200240, China
[2]School of Business Information Management,
Shanghai Institute of Foreign Trade, Shanghai 201620, China
yangnh@sjtu.edu.cn*

Abstract

A trust and reputation management framework for VANETs (Vehicular Ad Hoc Networks) is proposed. In the framework, a similarity mining technique is used for identifying similar messages or similar vehicles. And a reputation evaluation algorithm is proposed for evaluating a new vehicle's reputation based on the similarity theory. Similarities from different recommenders are used as weights for computing a vehicle's recommendation based reputation. An updating algorithm for reputations is proposed in the framework. The framework is applied to decide whether a message is trustworthy when a vehicle receives an event message.

Keywords: *trust, reputation, similarity, VANETs*

1. Introduction

Vehicular ad hoc networks (VANETs) [1] can broadcast real-time traffic event messages from one vehicle (or base station) to others through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication channels to avoid awful traffic situations in advance [2]. These messages can be alert signals about accidents, traffic congestion or information about traffic on a given route. So VANETs have drawn extensive attention [3-7] in recent years for their promising functions on traffic accident reduction, congestion reduction, and enhancement of comfortable driving experience. In VANETs, an inaccurate traffic event message will impact drivers' decisions, waste time and fuel, and even cause serious accidents [8].

Due to their open, distributed and dynamic nature, VANETs are vulnerable to various malicious attacks [4]. So security is an important concern in VANETs [9, 10]. For that purpose, each node can be authenticated [11, 12] using signature schemes [13] while sending information. However, a node may misbehave due to selfish reasons and might not send right information all the time. So it is more important to know the correctness of the message than the authority of the corresponding sender. In other words, it's important to evaluate the trustworthy of the received message and reputation of the sender to make decisions effective based on the received information.

Reputation is what is generally said or believed about a person's or thing's character or standing [14]. It is a subjective assessment for a node based on the user's own experience and recommendations from neighbors. A weight for a recommended reputation is depended on how much the receiver trusts the recommender. Trust is an evaluation of the confidence about the contents of the received message.

A good trust and reputation framework for VANETs should consider following issues simultaneously. Firstly, reputations for a new vehicle should be evaluated. Secondly, different weights should be assigned to reputations from different recommenders. Last but not least, reputations should be updated after each event message is confirmed.

This paper is extended from our previous work [15]. It proposes a trust and reputation management framework for VANETs. A similarity mining technique is used for identifying similarity among vehicles. A reputation evaluation algorithm is proposed for a new vehicle based on the similarity theory. The similarity evaluation method is based on the approach in [16]. Reputations of the recommenders are used as weights for computing indirect reputation of a message producer. An updating algorithm for reputations is proposed.

The rest of this paper is organized as follows. Section 2 surveys related work. Section 3 details the proposed trust and reputation management framework for VANETs. Experiments are described in Section 4. Section 5 concludes this paper.

2. Related Work

A lot of trust and reputation management approaches have been analyzed in the literatures [17, 18]. Three main classes of approaches for trust are identified [17]. They are direct experience based approaches, Trusted Third Party (TTP) based approaches and hybrid approaches that combine techniques of the previous two classes. Direct experience based approaches are based on evaluations given by the user's own direct experience with the target service [19]. Dragoni [17] points out that these approaches are not appropriate for open systems, since the service consumer can't evaluate a service with no direct experience. TTP approaches are based on the evaluation results provided by trusted party. Malik, *et al.*, [20] propose a reputation bootstrapping method based on the concept of community. They argue that services in a particular domain will aid each other in evaluating the initial reputation of the new service.

Hybrid approaches combine direct experience based approaches and TTP based approaches. The approach proposed in this paper belongs to this category. Jøsang, *et al.*, [21] combine Bayesian reputation systems with a trust model for evaluating the quality of service in a single framework. But it is based on a centralized and trusted reputation center [17]. Chen, *et al.*, [22] propose a reputation model for evaluating web services. The model incorporates four types of reputation including direct reputation, relationship reputation, witness reputation and sell-oneself reputation.

To facilitate the implementation of trust and reputation management in ad hoc networks, various trust and reputation metrics have been designed and integrated into various applications in the literature. Trust is combined with QoS requirements to act as the routing metric in wireless ad hoc networks in [23]. Zhang, *et al.*, [24] propose a formal study method for trust-based routing in wireless ad hoc networks. Mundinger et al. [25] build a stochastic process to formulate the behavior of the nodes in a mobile ad hoc network and derived a mean ordinary differential equation for misreport detection. Luo, *et al.*, [26] build a fuzzy logic reputation model to deal with the uncertainty and tolerance of imprecise data inputs in mobile ad hoc networks. Li and Shen [27] propose a hierarchical account-aided reputation management system (ARM) to efficiently and effectively provide cooperation incentives for the purpose of encouraging cooperative and deterring selfish behaviors in mobile ad hoc networks.

Various secure communication protocols [28] have been proposed to ensure message authentication and integrity for the purpose of alleviating fraud message problem in traffic application on VANETs. Raya, *et al.*, [29] propose a data-centric trust establishment framework for traffic safety application in VANETs. The method in [29] is used to evaluate the trust of received messages rather than the reputation of individual vehicle. Lo, *et al.*, [8] propose an event-based reputation system to provide accurate and reliable traffic information to drivers and resist the false alarm effect from fraud messages spread in the network. The mechanism in [8] can't provide real-time trust information. It also does not concern the reputation of the message producer.

Nepal, *et al.*, [30] propose a fuzzy trust evaluation approach. But they do not give an effect method for evaluating the trust of a new one. Shao, *et al.*, [16] propose a similarity computing algorithm for web services and their consumers based on Euclidean distance [31] theory. Consumers' similarities are used as weights of indirect experiences. Similarities between target web service and other ones are used as weights for QoS prediction of the target web service. The similarity computing algorithm proposed in [16] is used in this paper for evaluating message producers' similarities.

3. Trust and Reputation Management Framework

This section details our trust and reputation management framework for VANETs. Firstly, the message trustworthy model is introduced. Then similarity mining algorithm is proposed for repeaters and messages. Reputation evaluation for a message producer is proposed based on integrating of direct experience and recommendation. Trust and reputation will be updated after the validation of the message content is checked.

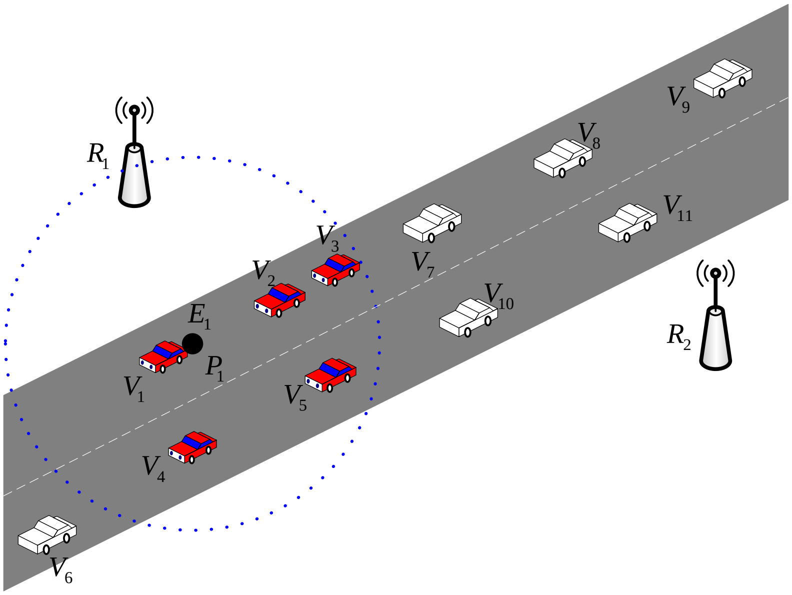

Figure 1. Event message dissemination model

3.1 Message Trustworthy Model

Figure 1 describes an event message disseminating model. In the time T_1 , the vehicle V_1 broadcasts a message to report an event E_1 in the position P_1. Vehicles (such as V_2 , V_3, V_4 and V_5) in the message transmission range of V_1 will receive the event message. The vehicle received the message will calculate the trust value of the message according to the method proposed in the following. If the trust value is not less than a predefined threshold, the received vehicle should take corresponding actions to the message and rebroadcast the message. Otherwise, the message will be discarded. The message trustworthy model, presented in Figure 1, consists of two clusters, “Vehicles” and “Messages”.

Definition 1. A message is a 4-tuple, $M = (I, E, L, T)$. I is the identification of the message producer. E is the event type, such as an alert signal, traffic congestion, *et al.*, $L = (Lat, Long)$ represents the latitude and longitude of the event. T is the time when the event was sensed or fabricated by the message producer.

Definition 2. A vehicle is a 3–tuple, $V = (I, C, V)$. I is the identification of the vehicle or its pseudonym which is used for privacy preserving [32]. C belongs to the vehicle’s types, which includes infrastructures, service cars, buses, taxies, trucks and sedan cars. $V = (S, D)$ is the velocity of the vehicle when it sent the message. S represents the speed and D represents the direction. D is described with the degree of departure from due north along the clockwise direction.

Different type vehicles have different initial reputation in the VANETs.

3.2 Similarity Mining

Lots of similarity mining approaches have been proposed by researchers. Euclidean distance [31] based similarity mining approach overcomes some disadvantages of other approaches, such as the collaborative filtering based method [33], when it is used to compute similarity between non-linear similar data. The similarity computing method used in this paper is developed from the method proposed in [16] which is based on Euclidean distance.

To simplify description, some objects are formally defined as follows. $M = \{m_1, m_2, \cdots, m_r\}$ is the set of messages. $V = \{v_1, v_2, \cdots, v_s\}$ is the set of vehicles.

At similar location and similar time, messages about the same event produced by the same vehicle usually hold similar trust values. In Table 1, all the messages are produced by the same vehicle and descript the same event. *Lat* and *Long* represent the latitude and longitude of the location where the message was generated. T is the time when the message was generated. V_T represents the historical trust value of the message given by the received vehicle. In order to evaluate the trust value of the message m_4, similarities between m_4 and other messages in Table 1 should be calculated.

Table 1. Properties of messages procedued by the same vehicle and their trust values for the event of congestion

	Lat	*Long*	T	V_T
m_1	31.220500	121.470800	00:00:45	0.2
m_2	31.220300	121.470500	10:00:45	0.6
m_3	31.220300	121.470100	17:35:41	0.95
m_4	31.220800	121.469800	09:15:49	

Vehicles belongs to the same class usually hold the similar reputation. For example, infrastructures at roadsides and service cars always hold high reputation values. When these vehicles sensed events, their speeds and directions are usually similar respectively. In order to calculate similarity between vehicles, Table 2 presents some examples for describing vehicles' states when they producing event messages. In Table 2, *S* represents speed and *D* represents the direction of the vehicle. The variable *R* represents the historical reputation for a vehicle corresponding to the given velocity. In order to evaluate the reputation of v_4 in Table 2, similarities between v_4 and other vehicles should be calculated.

Table 2. States of vehicles when producing event messages and their historical reputations

	S	*D*	*R*
v_1	28	180	0.96
v_2	58	136	0.78
v_3	36	226	0.90
v_4	50	316	

According to the approach proposed in [16], each row is regarded as a node. Thus, the similarity between two nodes can be represented by the Euclidean distance between them. The more distance two nodes are, the less similarity they become. Similarity between two nodes based on Euclidean distance is computed according to Eq. (1) which is proposed in [16].

$$w = \frac{1}{(\sum_{i=1}^{n}(X_i - Y_i)^2 / n)} \tag{1}$$

In Eq. (1), *X* and *Y* are vectors. X_i (or Y_i) represents the value of the *i*-dimension in the vector. For similarity calculation, times represented by *T* in Table 1 are divided into peak hours and non-peak hours. Times division for peak hours and non-peak hours can be adjusted according to the statistics for traffic conditions. A peak hour is represented by 1 and a non-peak hour is represented by 0 in Eq. (1).

3.3 Direct Experience Based Reputation

Whether the event described by the received message was really occurred will be checked when the receiver pass the location described by the message. A vehicle or its driver will give a reputation for the message producer after confirming the truth of the message. Let $r_{i,j}^{(n)}$ be the reputation value for the vehicle *j* given by the vehicle *i* after confirming the *N*-th event message produced by the vehicle *j*. After the total number of *n* event messages produced by the vehicle *j* have been confirmed successively by the vehicle *i*, the comprehensive reputation, which is represented as $R_{i,j}^{(n)}$, can be calculated by Eq. (2).

$$R_{i,j}^{(n)} = \begin{cases} \alpha R_{i,j}^{(n-1)} + (1-\alpha) r_{i,j}^{(n)}, & n > 1 \\ r_{i,j}^{(n)}, & n = 1 \end{cases} \tag{2}$$

In Eq. (2), α ($0 \le \alpha \le 1$) is a history factor. Encouragement and punishment factors for reputation are not considered in this paper for simplicity. Eq. (2) is also used as reputation updating formula for the vehicle *j* given by the vehicle *i*.

3.4 Recommendation Based Reputation

When the message receiver has no direct experience based reputation about the message producer, or in order to get much information about the reputation of the message producer, recommended reputations from other receivers are important. The receiver *i* can calculate the recommended reputation of the vehicle *j* based on recommendations from recommenders. The algorithm for recommendation based reputation is represented by Eq. (3).

$$C_{i,j} = \frac{\sum_{k=1..n,k\neq i} (w^{u}_{i,k} \times R_{i,k} \times R_{k,j})}{\sum_{k=1..n,k\neq i} (w^{u}_{i,k} \times R_{i,k})} \tag{3}$$

In Eq. (3), $C_{i,j}$ is the comprehensive recommended reputation of the vehicle *j* for the receiver *i*. $w^{u}_{i,k}$ is the similarity between the receivers *i* and *k*. $R_{i,k}$ is reputation evaluation of the vehicle *k* given by the vehicle *i*. $R_{k,j}$ is the direct experience reputation about the vehicle *j* given by vehicle *k*. *n* is the number of recommenders.

3.5 Reputation of a New Vehicle

If there is no recommender for the reputation of the vehicle *j* and no direct experience based reputation about the vehicle for the message receiver *i*. The vehicle *j* is regarded as a new vehicle for the message receiver in this situation. The reputation evaluation method for a new vehicle is based on the reputations of similar event messages produced by similar vehicles. Similarity between vehicles is also computed by Eq. (1).

The reputation of a new vehicle for the message receiver *i* can be calculated by Eq. (4).

$$R_{i,j} = \frac{\sum_{k=1..n,k\neq j} (w^{s}_{j,k} \times R_{i,k})}{\sum_{k=1..n,k\neq j} w^{s}_{j,k}} \tag{4}$$

In Eq. (4), *n* is the number of vehicles which belong to the same vehicle class with the new vehicle *j*, whose direct or recommended reputations can be got by the vehicle *i*. $w^{s}_{j,k}$ is the similarity value between the vehicles *j* and *k*. $R_{i,k}$ is the comprehensive reputation value of the vehicle *k* given by the vehicle *i* in the history.

For the first appeared vehicle belongs to a special class, its reputation is set to be 0.5 for the event message receiver. Reputations for infrastructures or public service vehicles in VANETs will be set a large value.

3.6 Trust Value for a Message

The trust value for an event message is a weighted average value of the direct experienced reputation and recommended reputation. It is calculated by Eq. (5).

$$V_{T}^{(i,j)} = \beta R_{i,j} + (1-\beta) C_{i,j} \tag{5}$$

In Eq. (5), β ($0 \leq \beta \leq 1$) is the weighting factor for reputation based on direct experience. $R_{i,j}$ is the direct experience based reputation for the vehicle *j* given by the message receiver *i* in history. $C_{i,j}$ is the comprehensive reputation of the vehicle *j* calculated based on the neighbors' recommendations for the message receiver *i*.

If the trust value of the received message is larger than a given threshold, the received vehicle will take actions according to the content of the message and rebroadcast the message. Or the message will be discarded.

3.7 Reputation Updating

After confirming whether the event disseminated by the message was really occurred, the message receiver will give a new reputation for the message producer. The comprehensive reputation in history will be updated according to Eq. (2). The updated comprehensive reputation includes the influence from the latest reputation given by the message receiver.

Reputation for the recommender given by the message receiver should also be updated according the degree of deviation between recommended reputation and the reputation given by the message receiver after confirming. Reputation updating method is proposed in Eq. (6).

$$R_{i,j}^{(n)} = \begin{cases} 0.5, & \text{n=0} \\ R_{i,j}^{(n-1)} - \left|R_{j,k} - R_{ik}\right| \times R_{i,j}^{(n-1)}, & \text{n>0 \& } \left|R_{j,k} - R_{ik}\right| \geq \delta \\ R_{i,j}^{(n-1)} + \dfrac{\left|R_{j,k} - R_{ik}\right|}{8} \times (1 - R_{i,j}^{(n-1)}), & \text{n>0 \& } \left|R_{j,k} - R_{ik}\right| < \delta \end{cases} \tag{6}$$

In Eq. (6), $R_{i,j}^{(n)}$ represents the comprehensive reputation value of the recommender *j* evaluated by the message receiver *i* after *n*-times interactions. $R_{j,k}$ is the reputation of the vehicle *k* recommended by the recommender *j*. R_{ik} is the reputation of the vehicle *k* given by the message receiver *i* after confirming the message. $R_{i,j}^{(0)}$ is the initial reputation value between vehicles. δ, $0 \leq \delta \leq 1$, is a boundary value for telling whether a recommender is honest or not. Eq. (6) shows that a recommender will get reputation slowly after providing honest recommended reputations continuously, but will lose reputation dramatically after giving a dishonest recommendation.

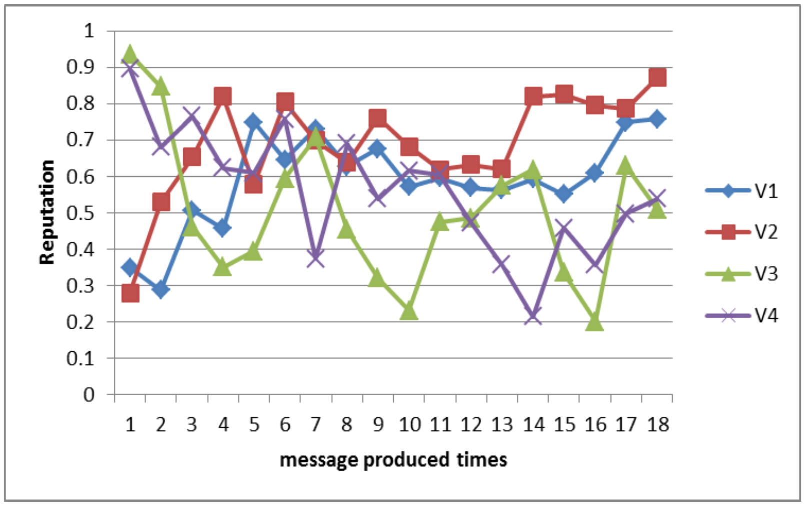

Figure 2. Reputation changing process

4. Experiment

The experiment is conducted on the computer with the CPU of Pentium(R) D 2.80GHz, 512 MB Memory, Microsoft Windows XP Professional Service Pack 3. The program is implemented by the Java language with JDK 6.0.

Properties of each vehicle or message are initialized with numbers generated randomly. Four vehicles are set initially. Figure 2 shows reputation changes of each vehicle updated by a message receiver after confirming.

5. Conclusion

Evaluating the trustworthiness of a vehicle in VANETs still remains as an open problem until now. Reputations play important roles in trustworthiness evaluation. They provide foundations for estimating the trustworthiness of a message or a vehicle based on historical information. This paper proposes a trust and reputation management framework for VANETs based on similarities between messages and similarities between vehicles. A similarity mining technique is used for identifying similarity among vehicles and messages. A reputation evaluation algorithm is proposed for a new vehicle based on the similarity theory. Similarities and reputations of recommenders are used as weights for computing comprehensive reputation for the message producer. An updating algorithm for reputation is proposed. The framework is applied to help the driver to decide whether he should believe the received message or not.

Acknowledgements

This work was supported by the NSF of China under grants No. 61173048 and 60973107, Shanghai 085 Project for Municipal Universities, Innovation Program of Shanghai Municipal Education Commission under grant No. 12ZS170, Shanghai special scientific research funds for selecting and cultivating excellent young teachers in colleges and universities under grant in 2012.

References

[1] J. J. Blum, A. Eskandarian and L. J. Hoffman, "Challenges of intervehicle ad hoc networks", IEEE Transactions on Intelligent Transportation Systems, vol. 5, no. 4, **(2004)**, pp. 347-351.

[2] S. Biswas, R. Tatchikou and F. Dion, "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety", IEEE Communications Magazine, vol. 44, no. 1, **(2006)**, pp. 74-82.

[3] C. Langley, R. Lucas and H. Fu, "Key management in vehicular ad-hoc networks", IEEE International Conference on Electro/Information Technology, 2008(EIT 2008), **(2008)** May 18-20, pp. 223-226.

[4] G. Yan, S. Olariu and M. C.Weigle, "Providing VANET Security through active positon detection", Computer Communications, vol. 31, no. 12, **(2008)**, pp. 2883-2897.

[5] W. Chen, R. K. Guha, T.J. Kwon, J. Lee and Y. -Y. Hsu, "A survey and challenges in routing and data dissemination in vehicular ad hoc networks", Wireless Communications and Mobile Computing, vol. 11, no. 7, **(2011)**, pp. 787-795.

[6] F. J. Martinez, C. K. Toh, J. -C. Cano, C. T. Calafate and P. Manzoni, "A survey and comparative study of simulators for vehicular ad hoc networks (VANETs)", Wireless Communications and Mobile Computing, vol. 11, no. 7, **(2011)**, pp. 813-828.

[7] P. Kamat, A. Baliga and W. Trappe, "An identity-based security framework For VANETs", Proceedings of the 3rd international workshop on Vehicular ad hoc networks, **(2006)**; Los Angeles, CA, USA: ACM, pp. 94-95.

[8] N. -W. Lo and H. -C. Tsai, "A reputation system for traffic safety event on vehicular ad hoc networks", EURASIP Journal on Wireless Communications and Networking 2009, **(2009)** February, pp. 1-10.

[9] P. Golle, D. Greene and J. Staddon, "Detecting and correcting malicious data in VANETs", Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, **(2004)**; Philadelphia, PA, USA: ACM, pp. 29-37.

[10] T. Leinmuller, E. Schoch and C. Maihofer, "Security requirements and solution concepts in vehicular ad hoc networks", Fourth Annual Conference on Wireless on Demand Network Systems and Services, 2007(WONS '07), **(2007)**, pp. 84-91.

[11] T. W. Chim, S. M. Yiu, L. C. K. Hui and V. O. K. Li, "MLAS: Multiple level authentication scheme for VANETs", Ad Hoc Networks, vol. 10, no. 7, **(2012)**, pp. 1445-1456.

[12] M. Riley, K. Akkaya and K. Fong, "A survey of authentication schemes for vehicular ad hoc networks", Security and Communication Networks, vol. 4, no. 10, **(2011)**, pp. 1137-1152.

[13] Y. Jiang, M. Shi, X. Shen and C. Lin, "BAT: A robust signature scheme for vehicular networks using Binary Authentication Tree", IEEE Transactions on Wireless Communications, vol. 8, no. 4, (2009), pp. 1974-1983.

[14] A. Jøsang, R. Ismail and C. Boyd, "A survey of trust and reputation systems for online service provision", Decision Support Systems, vol. 43, no. 2, **(2007)**, pp. 618-644.

[15] N. Yang, X. Chen and H. Yu, "A Reputation Evaluation Technique for Web Services", International Journal of Security and Its Applications, vol. 6, no. 2, **(2012)**, pp. 329-334.

[16] L. Shao, Z. Li, J. Zhao, B. Xie and H. Mei, "Web Service QoS Prediction Approach", Journal of Software, vol. 20, no. 8, (in Chinese with English abstract) **(2009)**, pp. 2062-2073.

[17] N. Dragoni, "A Survey on Trust-Based Web Service Provision Approaches", Proceedings of the 2010 Third International Conference on Dependability, **(2010)** July 18 - 25; Venice/Mestre, Italy: IEEE Computer Society, pp. 83-91.

[18] S. Ruohomaa and L. Kutvonen, "Trust Management Survey", Proceedings on Third International Conference on Trust Management (iTrust 2005), **(2005)** May 23-26; Paris, France: Springer Berlin / Heidelberg, pp. 77-92.

[19] A. S. Ali, S. A. Ludwig and O. F. Rana, "A Cognitive Trust-Based Approach for Web Service Discovery and Selection", Proceedings of the Third European Conference on Web Services (ECOWS 2005), **(2005)** November 14-16; Växjö, Sweden: IEEE Computer Society, pp. 38-49.

[20] Z. Malik and A. Bouguettaya, "Reputation Bootstrapping for Trust Establishment among Web Services", IEEE Internet Computing, vol. 13, no. 1, **(2009)**, pp. 40-47.

[21] A. Jøsang, T. Bhuiyan, Y. Xu and C. Cox, "Combining Trust and Reputation Management for Web-Based Services", Proceedings of the 5th international conference on Trust, Privacy and Security in Digital Business, **(2008)** September 4-5, Turin, Italy: Springer-Verlag, pp. 90-99.

[22] C. HaiBao, Z. ShengHui and C. GuiLin, "A reputation model for evaluating Web services", Proceedings of Fourth International Conference on Communications and Networking in China (ChinaCOM 2009), **(2009)** August 26-28; Xi'an, China: IEEE Computer Society, pp. 1-10.

[23] M. Yu and K. K. Leung, "A trustworthiness-based QoS routing protocol for wireless ad hoc networks", IEEE Transactions on Wireless Communications, vol. 8, no. 4, **(2009)**, pp. 1888-1898.

[24] C. Zhang, X. Zhu, Y. Song and Y. Fang, "A formal study of trust-based routing in wireless ad hoc networks", Proceedings of the 29th conference on Information communications, **(2010)** March 15-19; San Diego, California, USA: IEEE Press, pp. 2838-2846.

[25]J. Mundinger and J. -Y. L. Boudec, "Analysis of a reputation system for Mobile Ad-Hoc Networks with liars", Performance Evaluation, vol. 65, no. 3-4, **(2008)**, pp. 212-226.

[26] J. Luo, X. Liu and M. Fan, "A trust model based on fuzzy recommendation for mobile ad-hoc networks", Computer Networks, vol. 53, no. 14, **(2009)**, pp. 2396-2407.

[27] Z. Li and H. Shen, "A hierarchical account-aided Reputation Management system for large-scale MANETs", 30th IEEE International Conference on Computer Communications (INFOCOM 2011), **(2011)** April 10-15; Shanghai, China: IEEE Press, pp. 909-917.

[28] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung and J. -P. Hubaux, "Secure vehicular communication systems: design and architecture", IEEE Communications Magazine, vol. 46, no. 11, **(2008)**, pp. 100-109.

[29] M. Raya, P. Papadimitratos, V. D. Gligor and J. -P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks", 27th IEEE International Conference on Computer Communications (INFOCOM 2008), **(2008)** April 13-18; Phoenix, AZ, USA: IEEE Press, pp. 1238-1246.

[30] S. Nepal, W. Sherchan, J. Hunklinger and A. Bouguettaya, "A Fuzzy Trust Management Framework for Service Web", Proceedings of the IEEE International Conference on Web Services (ICWS 2010), **(2010)** July 5-10; Miami, FL, USA: IEEE Computer Society, pp. 321-328.

[31] E. Keogh and S. Kasetty, "On the Need for Time Series Data Mining Benchmarks: A Survey and Empirical Demonstration", Data Mining and Knowledge Discovery, vol. 7, no. 4, **(2003)**, pp. 349-371.

[32] G. Calandriello, P. Papadimitratos, J. -P. Hubaux and A. Lioy, "Efficient and robust pseudonymous authentication in VANET", Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, **(2007)**; Montreal, Quebec, Canada: ACM, pp. 19-28.

[33] J. L. Herlocker, J. A. Konstan, A. Borchers and J. Riedl, "An algorithmic framework for performing collaborative filtering", Proceedings of the 22nd annual international ACM SIGIR conference on Research and development in information retrieval, **(1999)** August 15-19; Berkeley, California, United States: ACM, pp. 230-237.

Authors

Nianhua Yang received his BSc in Management Information Systems from Beijing Information Technology Institute, China, in 2001, MSc and PhD in Computer Science and engineering from East China University of Science and Technology in 2004 and 2011 respectively. He is now a postdoctor in department of Computer Science & Engineering at Shanghai Jiaotong University. His current research interests include wireless ad hoc networks, VANETs, reputation management, privacy preserving in wireless networks, formal methods, cloud computing, *et al.*