International Journal of Engineering & Technology, 7 (4) (2018) 4073-4078

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet. v7i4.15822
Research paper

Trusted management for VANETs using vehicular social Behavior

Muhammed Abaid Mahdi *

University of Babylon
**Corresponding author E-mail:* wsci.muhammed.a@uobabylon.edu.i

Abstract

Information sharing is the main task of designing the most Vehicular Ad hoc Networks (VANETs). However, determining a degree of the trustworthiness for the receiving information is still a big challenge. This paper tries to bridge social networks with vehicular networks to utilize the social relationships among vehicles in increasing the trust level of information. While vehicles are immigrating to the next smart generation, considering vehicles as social objects may be justifiable. Indeed, due to advanced technologies vehicles can wirelessly contact with each other. Moreover, a level of intelligence those vehicles have easies the task of making decisions. The suggested method, firstly, gathers vehicles in permanent vehicular social groups (formal groups) depending on their social behavior and temporary vehicular social groups (casual groups) depending on the direction and the communication range. This grouping process assumes that vehicles in a formal group are tied with the strong social relationship. On the other hand, a casual group may consist of vehicles from different formal groups. When the source of information which is a vehicle that detects an event, shares a piece of information (the event), all members of its formal group can vote for this information. So, the trustworthiness degree of the shared information will be increased depending on the number of its votes. It means that the high number of votes the high level of trust. Eventually, each piece of information would be adopted when trusting votes of this information exceed a specific threshold. The results will discuss the main factors that affect the suggested method.

Keywords: *Casual Grouping; Formal Grouping; SNs; Trusted Management; VANETS; VSNS.*

1. Introduction

Several papers have been published to improve the transportation systems by designing Vehicular Ad hoc Networks (VANETs). Advanced technologies encourage researchers to pay attention for developing intelligent transportation systems where vehicles, nowadays, have reasons to be smart objects. Indeed, they can communicate with each other and communicate with the roadside unites. Vehicle to Vehicle (V2V), Vehicle to road side (V2R), and (R2R) are the main forms of the communications in VANETs [1]. Moreover, vehicles have some intelligence due to having CPU and memory. So, this feature makes vehicles able to make decisions and store their experience. In this context, it has been argued that vehicles can be considered as social objects as long as they can behave as smart objects. On the other side, Information diffusion is a main task for which the most VANETs are designed. Each vehicle which detects an event can share a piece of information about that event with others. There are four types of receiving messages in VANETS. The most well-known type is warning messages. These messages include information related to avoid the critical emergences for example traffic jam, natural disaster. The second type is that information which is used in entertainment applications when passengers share videos or games with each other during traveling. The third one is routing massages that are used in routing packets in VANETs such as source ID, position, direction and etc. the last type is related to recommendation systems, when vehicles recommend for example a gas station or a restaurant for other vehicles.

However, ensuring trusting messages is still a big issue that needs to be considered [2]. Evaluating the quality of the receiving messages may increase the compromise of the entire network. This process is to avoid false messages that sent by malicious vehicles. In this direction, this paper suggests creating social friendships among vehicles to strengthen their ties. Nonetheless, there are some research questions that need to be addressed to have a clear picture. Firstly, how vehicles can be gathered in social groups needs to be brought to light. Then, there is a need to explain how those social groups of vehicles will contribute to solve the problem of trust management in VANETs.

This paper is arranged in several sections as well as the introduction. The next section is dedicated to discuss the project's society impact and motivations. The third section is to survey the most literatures that have been done so far. This section is divided into two main subsections. The first one is related to works that have been linking Social Networks (SNs) and Vehicular Networks (VNs) whereas the second one is to review the most methods of managing trust in VANETs. The suggested methods and algorithms will be explained in the fourth section. A new research direction Vehicular Social Networks (VSNs), which is suggested to contribute in solving the problem of trust management in VANETs, will be highlighted in this section. The fifth section is to show and analyze the obtained results. Eventually, all nutshells of this project will be summarizes in the last section it is named conclusions.

2. Aims and challenges of the project

Since it is Internet of Things (IoTs) era, cities have been going to be smart. One of the most subclass of IoTs is Internet of Vehicles (IoVs) [3]. The communications of smart vehicles contribute in improving the transportation systems. They are undergoing a qualitative leap due to advanced technologies. Therefore, utilizing this scenario attracts researcher's attention to develop the intelligent transportation systems (ITSs). One of the most issues in this research direction is how to trust receiving messages in VANETs [4]. However, modeling trust management in VANETS may present several unique challenges [5]. Indeed, due to some features of VANETs, managing trust for such networks may be difficult task. One of the most constraints that make this task not easy is high mobility of VANETs. Vehicles are roaming around with high speed particularly in highway scenario. In the context of real time application, this rapidly change in topology of the network may make the reacting time to an imminent situation a critical time. Another issue may emerge which is related to the fact that VANET is a very large network. Especially at the urban scenario where number of peers in such these networks may exceed thousands. In peak time as rush hours this number may exacerbate. This high number of peers causes the network congestion when the peers compete to have a communication channel. Therefore there is a real need to design an intelligent and scalable communication system to overcome this challenge. Further, due to decentralization that characterizes VANETs there is no guarantee to communicate with the same vehicle in the next time. So there is much suspicion, in decentralized networks, to decide which peer to trust. The last challenge is related to the information nature of such these networks. In VANETs, a piece of information is not valid for long time. For example, a road may be free fifteen minutes ago but it is busy now. It means information in VANEs may be expired and this brings to light an important challenge that is how to evaluate information in a particular context. These challenges previously mentioned need to be addressed when trusted management for VANETs is modelled.

This paper tries using the concepts of SNs to solve trust management issue in VANETs. By creating friendships among vehicles the trustworthiness degree will be increased. Vehicles that behave a similar behavior can be grouped in permanent social groups. This social grouping process may facilitate verifying a piece of information. Vehicles that know the source of information can vote behalf this information. Combining both SNs and VNs leads to emerge a new promising research field which is Vehicular Social Network (VSN) [6]. Many Novel applications of VSNs can be derived from VNs applications and have a significant impact on society and the transportation systems. Fig 1 shows the most applications of VSNs.

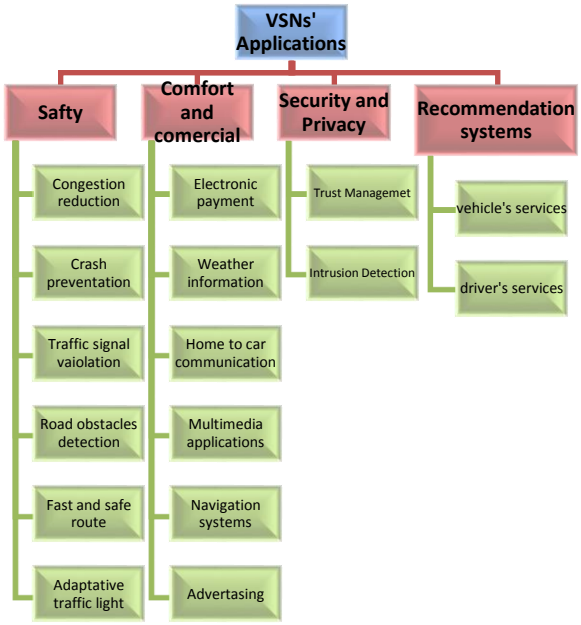


Fig. 1: Applications of VSNS.

3. Literature review

Even though there are several literatures have bridged SNs and VNs, this paper presents a new model to link them to increase the trustworthiness degree For VANETs. Moreover, it suggests a way to gather vehicles in social groups to strengthen the social ties among vehicles. In the next subsections, the most related works will be brought to light.

3.1. Bridging SNs and VNs

The entire document should be in Times New Roman. The font sizes to be used are specified in Table 1.

Many papers have argued that linking SNs and VNs may have positive effect on improving VANETs. Security and privacy challenges are discussed in [7] utilizing the viewpoint of SNs. On the other hand, a new novel scheme has been suggested in [8] to overcome oversampling and cascading problems.

A new video sharing method has been presented in [9] to enable commuters in spreading their videos during traveling. Recommendation systems also have been discussed exploiting concepts of SNs. In the similar context, authors in [10] have proposed a recommendation system for joining passengers with their friends while trip. Besides, Analyzing Topologies of Wireless Sensors Networks (WSNs) and VNs has been presented in [11] using centrality metrics.

Table 1: Related Works to Bridge SNS and VNS

	Ref	Security Issues	Managing trustworthiness	Videos diffusion	Recommendation systems	Controlling topologies
Linking VNs and SNs	[7]	✓				
	[8]	✓	✓			
	[9]			✓		✓
	[10]				✓	
	[11]					✓

3.2. Trusted management for VANETS

There is no clear definition for trust in networks [4], even though the term of trust has been borrowed from social sciences. However, in the field of mobile networks researchers have used the trust to enhance the security of those networks. Because of lack of centralization, VANETs are difficult to be secured using traditional security mechanisms [4]. So there is a need to highlight new techniques to improve the security in VANETs. A new trust model has been suggested in [12] to help a normal node to select a right choice and to avoid harmful vehicles. Providing a reliable safe traffic has been presented in [13] by designing a trust model. According to the previous sources, trusted management can be classified into three types. These are data centric, entity centric, and hybrid. The first type considers that data is the main object of the trust model.in such these models, the main task is to focus on data instead of entities. In these types of models, evaluating the re-

ceived information is required to give a trust level for each piece of received information [14]. On the other hand, entity centric types focus on trustworthiness of peers (vehicles). In such these models, historical information about the senders (vehicles) is needed to achieve the goals. Due to high mobility such this information could be difficult to collect. Moreover, measuring trustworthiness of data is still a challenge even if the sender is trustworthy [14]. For this reason, focusing on both data and entity is desired to have high level of trust. Therefore, hybrid models have been suggested for this purpose [15].

To summarize the models of trusts in VANETs, table 2 includes the most related works and the techniques used in each.

Table 2: Related Works to Trust Models in VANETs

	Ref	Using data centric	Using entity centric	Using hybrid	Using reputation concept	Using concepts of SNs
Trust management in VANETs	[16, 17]	✓				
	[18]	✓				
	[19, 20]		✓		✓	
	[12]		✓		✓	
	[21]	✓	✓	✓	✓	
	[8]		✓		✓	✓

4. Methodologies and implementation

4.1. Modelling mobility of VSNs

Since VANETs are complex and multi-agent systems [22], modelling mobility for such these systems need to be carefully considered. Complex Agent Network (CAN) is a term which combines both Agent Based Model (ABM) and Complex Network (CN) [23]. ABM can model the interaction among vehicles and other agents such as traffic lights and Road Side Units (RSUs). The latter agent is added to improve the connectivity of the network [24]. On the other hand, CN can give a clear picture to the all social groups of the entire network [23]. So, it is believed that combination of both ABM and CN may precisely model mobility of VSNs. For this reason, this paper model the interactions of agents (vehicles, RSUs, and Traffic lights) using ABM and model the Social groups of Vehicles Using CN. In this model, each agent is defined as some parameters and some actions. Each action is depended on the parameters of the neighboring agents. Although this multi-agent model can arrange the relations among agents, it is still not fair enough to give comprehensive picture that describe the status of social groups in the entire system where some social behavior of vehicular groups need to be addressed. For example, knowing which giant group is essential to spread information. Moreover, some metrics of groups are also important such as density, diameter, and size of group. For that, CN is available to clearly describe the social groups of vehicles.

4.2. Grouping vehicles

The key characteristic of VSNs is how to gather vehicles in social groups. We suggested two main algorithms for this purpose [6]. Algorithm1 is Formal Social Grouping Algorithm (FSGA) attempts to strength the social ties of vehicles that have a similar social behavior. It permanently group vehicles in permanent groups. All vehicles that have similar daily behavior can be friends. For example vehicles that are daily traveling or parking at the same social place can be gathered in permanent social group. Another example is that vehicles of persons who work at the same company can be gathered in a formal social group. So vehicles of university staff absolutely will be gathered in formal social groups as long as these vehicles see each other frequently. FSGA is illustrated in[6] .

On the other hand, designing the Casual Social Grouping Algorithm (CSGA) is to gather vehicles that are not necessary to know each other. Just vehicles travel through a same direction and they are in a specific geographic area (communication range), they will be clustered in a casual group. Once a vehicle leaves a casual group due to changing its direction or its speed, it will kill its link. For this reason, such these groups will be temporary and there are no strong ties as formal groups. Algorithm2 CSGA is shown in [6]. This process of grouping is similar to the way by which people create their social relations. They have permanent relations with their colleagues and family. In the same time, they have temporary relations when they meet other people at the bus stations for instant. Sharing information will be more trusted in formal groups than in casual groups.

4.3. Trust management model for VANETS

After grouping process vehicles have been tied in social friendships. Hybrid trust model is designed for VSNs. Each entity (vehicle) has a parameter which is associated with to define trust degree (Ƞi) of that vehicle (vi). In similarity, each piece of information also has a parameter to define trust level (λ). Each vehicle (the source) that detects an event will try to share this information with their neighbors using the contagion model [25]. Each message is included id of the source and its position as a header. Basing on Ƞ of the source, vehicles that know the source will vote for the information. This positive voting will increase λ of the received information. When λ exceeds a specific threshold (t) this information will be adopted by all vehicles in a certain casual group. For more details, there is a need to define the assumptions of the suggested trust model. Let assuming N is a number of agents (vehicles) in the model. First of all, all vehicles will be grouped in social communities (formal groups) as previously discussed. Let assume F is the number of formal groups depending on social behavior of vehicles and C is the number of casual groups. Remember $F\ and\ C$ are both variable. Each formal group size $Z(G_{formal})$ is ranging from1 $into\ N$. Each vehicle $v_i \in N$ will be assigned to a suitable formal group. The v_i also will be clustered in a casual group according to its position and direction. It is not necessary that $F = C$ it also may be $v_i \in$ formal group and casual group at the same time. Indeed, these two grouping algorithms are already separated from each other. Now let assume the detector vehicle (the source) is s. Then this vehicle will be admin (cluster head) of its casual group. It then will share the information with its neighbors using contagion model. The first vehicle receives the information in each casual group will be the admin for that casual group. The admin will ask all its neighbors (members of its casual group) whether they know the source. If a vehicle knows the source (they are in the same formal group and trust degree (Ƞsource>= threshold), it will vote for the information and increase λ for that information. If λ exceeds the threshold t then this information will be adopted by other vehicles. Eq1 is to calculate t,

$$t = 0.20 * SZ\big(Formal\ group\ (s)\big) \quad (1)$$

SZ is the size of group of s and s is the source vehicle that detects the event.

Below the steps of the hybrid trusted management for VSN are illustrated.

Algorithm Hybrid Trusted Management Algorithm (HTMA)

Step1: Let N the set of vehicles (v_i where i= 1 to N) in urban region

Step2: Let t the threshold of trusted level of information

Step3: Let S the set of sources and set I_j=0 for s ∈S and λ=0. Initially S = {s}

Step4: Begin

Step5: Group vehicles using algorithms 1 and 2

Step6: While not all friends in the formal group (S) have not received the message Do

Step7: for all s ∈S will send the message to its neighbors

Step8: each received vehicle v_i will vote if $v_i \in formal\ group\ of\ s$ then λ=λ+1

Step9: End for step7

Step 10: if λ>=t then adopt the message

Step11: END.

5. Results and analysis

5.1. Social groups of vehicles

To test the proposed trusted model, defining some assumptions is required. Table 3 shows some parameters that are set using NetLogo ver. 5.3.1 [26].

Table 3: Parameters Assumptions of Simulation

Number of vehicles (N)	50,100, and 200
Scenario	Urban
Wireless standard technology	IEEE 802.11p
Number of streets	6
Communication range (R)	15,30, and 100
Speed	0-60 km/h
Number of runs	10
Number of formal groups	7
Number of casual groups	Variable

All vehicles that are in the same communication range and they travel through the same direction will be grouped in in a casual groups. So the number of casual groups mainly depends on two factors. These are communication range R and Direction. Figure2 illustrates the effect of N and R on the grouping process. This figure is obtained from GraphStream [27] which is a java library to analysis graphs.

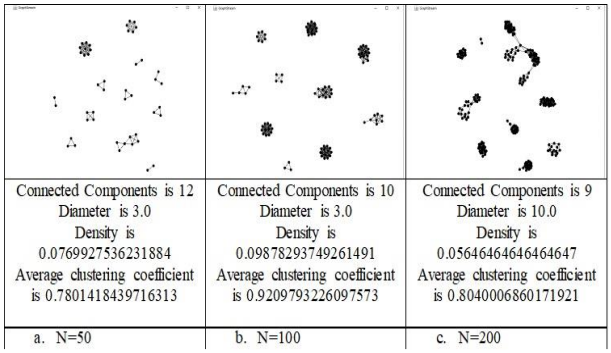


Fig. 2: (A, B) Graphs and Metrics to Analyse the Network when R=100m and N=50, and N=50,100, and 200.

On the other side, the number of links is shown in figure 3 which are created among vehicle in the entire network

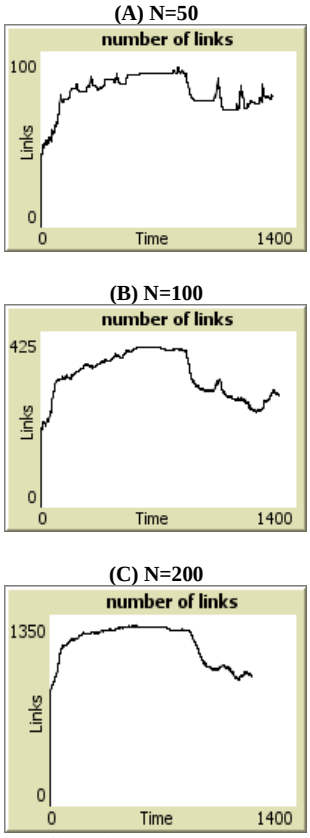
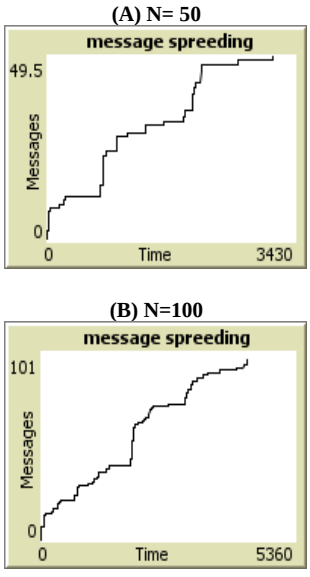


Fig. 3: (A-C) Effect of Density on the Number of Links.

To share information the contagion model is used. Eq2 shows the primary parameters to diffuse information using the contagion model. It is borrowed from [25].

$$\frac{dx(t)}{dt} = \beta_{for}\, x(t) + \beta_{cas} x(t)(1 - x(t)) \quad (2)$$

a) Where x(t) is a fraction of vehicles that adopt the given information at time t. β_{for} is the rate of vehicles that have received the information from their friends in formal groups. The parameter β_{cas} is the rate of vehicles that have obtained the information from their friends in the casual groups. The number of messages which are shared is shown in figure 4.



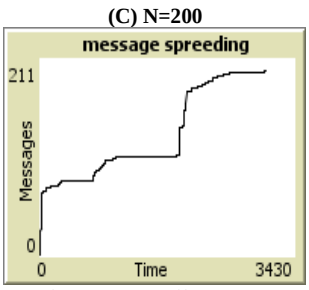


Fig. 4: (A-C) Number of Messages Diffused Using the Contagion Model with Different Density.

5.2. Testing trusted management model

Ten messages are shared to test the trusted management model on the network. In this diffusion process, different vehicles are used as sources. Some of them have already gathered in formal social groups to be considered as trusting vehicles. On the other side, others are selected to be malicious vehicles which do not belong to any social group. The number of adopted messages and the number of votes that exceed the t are shown in figure 5, whereas figure 6 illustrates the number of rejected messages that do not exceed the t.

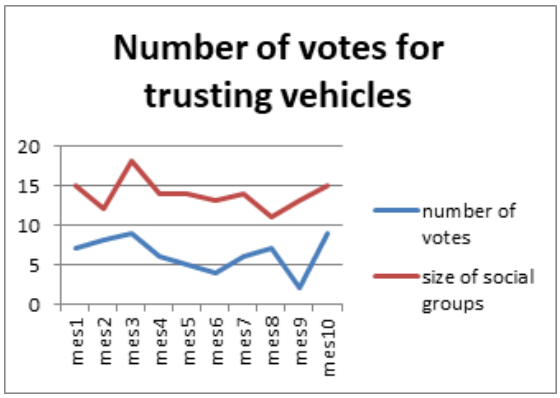


Fig. 5: The Number of Votes to Adopt Messages form Trust Vehicles.

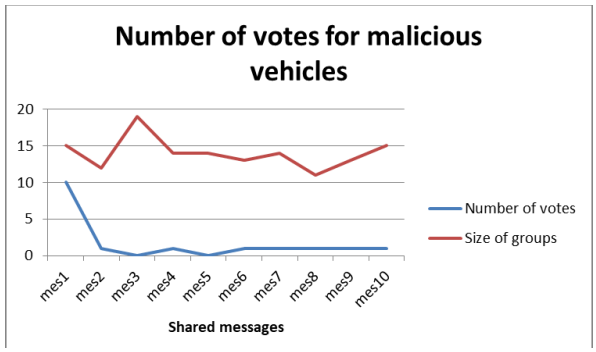


Fig. 6: The Number of Votes to Reject Messages form Malicious Vehicles.

As it is shown in figure 5 the number of votes is higher for trusting sources. It is approximately the half size of social groups. That means the most social friends in each social group will vote for trusting vehicles. As is shown in figure 5 there are nine messages are adopted whereas only one message (message 9) is rejected. On the other hand, malicious sources will not obtain votes. Grouping vehicles in social communities will help in increasing the trust of the sources of information. It is clear, all messages are rejected and only one message (message1) is adopted.

6. Conclusion

As trusted management for VANETs is an important research direction, real attention is required to pay to this challenge. High mobility and large network are features; VNs have, make this task difficult. This paper strongly believes that using the concepts of SNs may have a significant effect on contributing to solve this issue. VSN is a new multidisciplinary research direction that can link both SNs and VNs to regard vehicles as social objects. This VSN can increase the trust among vehicles that are gathered in social communities. Basing on this assumption, the shared messages can be filtered to detect undesired messages and to adopt the desired messages.

Acknowledgement

This work is supported by College of Science for Women/ University of Babylon.

References

[1] S. T. Hasson and M. A. Mahdi, "A Developed Realistic Urban Road Traffic in Erbil City Using Bi-directionally Coupled Simulations," Qalaai Zanist Scientific Journal,, vol. 2, no. 2, pp. 16-27, 2017.

[2] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," IEEE Access, vol. 4, pp. 9293-9307, 2016. https://doi.org/10.1109/ACCESS.2016.2645452.

[3] M. A. Mahdi and S. T. Hasson, "A Contribution to the Role of the Wireless Sensors in the IoT Era," Journal of Telecommunication, Electronic and Computer Engineering, vol. 9, no. 2-11, pp. 1-6, 2017 2017.

[4] S. A. Soleymani et al., "Trust management in vehicular ad hoc network: a systematic review," EURASIP Journal on Wireless Communications and Networking, vol. 2015, no. 1, p. 146, 2015. https://doi.org/10.1186/s13638-015-0353-y.

[5] J. Zhang, "A survey on trust management for vanets," in Advanced information networking and applications (AINA), 2011 IEEE international conference on, 2011, pp. 105-112: IEEE. https://doi.org/10.1109/AINA.2011.86.

[6] M. A. Mahdi and S. T. Hasson, "Grouping vehicles in Vehicular Social Networks," Kurdistan Journal of Applied Research, vol. 2, no. 3, 2017-08-27 2017.

[7] L. A. Maglaras, A. H. Al-Bayatti, Y. He, I. Wagner, and H. Janicke, "Social internet of vehicles for smart cities," Journal of Sensor and Actuator Networks, vol. 5, no. 1, p. 3, 2016. https://doi.org/10.3390/jsan5010003.

[8] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs," Peer-to-Peer Networking and Applications, vol. 7, no. 3, pp. 229-242, 2014. https://doi.org/10.1007/s12083-012-0136-8.

[9] K. M. Alam, M. Saini, D. T. Ahmed, and A. El Saddik, "VeDi: A vehicular crowd-sourced video social network for VANETs," in Local Computer Networks Workshops (LCN Workshops), 2014 IEEE 39th Conference on, 2014, pp. 738-745: IEEE.

[10] A. Elbery, M. ElNainay, F. Chen, C.-T. Lu, and J. Kendall, "A carpooling recommendation system based on social vanet and geosocial data," in Proceedings of the 21st ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, 2013, pp. 556-559: ACM. https://doi.org/10.1145/2525314.2525327.

[11] A. Papadimitriou, D. Katsaros, and Y. Manolopoulos, "Social network analysis and its applications in wireless sensor and vehicular networks," in International Conference on e-Democracy, 2009, pp. 411-420: Springer.

[12] X. Li, J. Liu, X. Li, and W. Sun, "RGTE: A reputation-based global trust establishment in VANETs," in Intelligent Networking and Collaborative Systems (INCoS), 2013 fifth International Conference on, 2013, pp. 210-214: IEEE. https://doi.org/10.1109/INCoS.2013.91.

[13] N. Bißmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for vanets based on mobility data plausibility," in Proceedings of the ninth ACM international workshop on

Vehicular inter-networking, systems, and applications, 2012, pp. 73-82: ACM. https://doi.org/10.1145/2307888.2307902.
[14] J. Zhang, "Trust management for VANETs: challenges, desired properties and future directions," International Journal of Distributed Systems and Technologies (IJDST), vol. 3, no. 1, pp. 48-62, 2012. https://doi.org/10.4018/jdst.2012010104.
[15] J. Grover, M. S. Gaur, and V. Laxmi, "Trust establishment techniques in VANET," Wireless Networks and Security, pp. 273-301, 2013. https://doi.org/10.1007/978-3-642-36169-2_8.
[16] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, 2008, pp. 1238-1246: IEEE.
[17] H. S. Basheer, C. Bassil, and B. Chebaro, "Toward using data trust model in VANETs," in Applied Research in Computer Science and Engineering (ICAR), 2015 International Conference on, 2015, pp. 1-2: IEEE. https://doi.org/10.1109/ARCSE.2015.7338136.
[18] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in International Conference on Network and System Security, 2013, pp. 94-108: Springer. https://doi.org/10.1007/978-3-642-38631-2_8.
[19] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 41, no. 3, pp. 407-420, 2011. https://doi.org/10.1109/TSMCC.2010.2084571.
[20] P. T. N. Diep and C. K. Yeo, "A trust-privacy framework in vehicular ad hoc networks (VANET)," in Wireless Telecommunications Symposium (WTS), 2016, 2016, pp. 1-7: IEEE. https://doi.org/10.1109/WTS.2016.7482038.
[21] Y.-M. Chen and Y.-C. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," Journal of Communications and Networks, vol. 15, no. 2, pp. 153-163, 2013. https://doi.org/10.1109/JCN.2013.000028.
[22] S. Hiroki, "<Introduction to the Modeling and Analysis of Complex Systems>," New York: Open SUNY Textbooks, 2015.
[23] S. Mei, N. Zarrabi, M. Lees, and P. M. Sloot, "Complex agent networks: An emerging approach for modeling complex systems," Applied Soft Computing, vol. 37, pp. 311-321, 2015. https://doi.org/10.1016/j.asoc.2015.08.010.
[24] W. Shanshan and Z. Chunxiao, "NetLogo Based Model for VANET Behaviors Dynamic Research," in Intelligent System Design and Engineering Applications (ISDEA), 2013 Third International Conference on, 2013, pp. 990-993: IEEE. https://doi.org/10.1109/ISDEA.2012.236.
[25] A. Louni and K. Subbalakshmi, "Diffusion of information in social networks," in Social Networking: Springer, 2014, pp. 1-22.
[26] NetLogo. (2017, 10 April). Available: https://ccl.northwestern.edu/netlogo/
[27] GraphStream. (2017, 30 March). Available: http://graphstream-project.org.