A SURVEY ON VANET BASED ON REGIONAL BLOCKCHAIN FOR VECHICULAR NETWORKS

Ms.S.SUNDHARAMBAL

Department of computer science and engineering,

Sri ManakulaVinayagar Engineering College,

Madagadipet, Puducherry.

Sundhari81195@gmail.com

Dr.V. VIJAYA KUMAR

Department of computer science and engineering,

Sri ManakulaVinayagar Engineering College,

Madagadipet, Puducherry.

vijayakumarv@smvec.ac.in

ABSTRACT

Trust establishment in vehicular ad hoc networks (VANETs) is a challenging task dueessentially to the high speed of vehicles, the long distances, and the network topology dynamics.Furthermore, applications context evolves quickly at the same time that the lifetime validity of data messagesis short. In this paper, we set up a newdistributed trust computing framework tailored toVANETs characteristicsand aiming to solve the aforementioned challenges. The proposed framework is based on the investigationof the direct experience between neighboring vehicles without using any recommendation system. We alsopropose a tier-based messages dissemination technique in order to efficiently detect eavesdropped messagesand fake events. Each vehicle checks the authenticity of the received data messages and maintains a trustvalue for each of its neighbors. We analytically model the trust metrics evolution of malicious vehicles.Extensive simulations are conducted to show the validity of the proposed model and evaluate the efficiencyof the proposed trust computing framework.

Keywords: Vehicular ad hoc networks, trust computing, analytical modeling, simulation

INTRODUCTION

The number of vehicles on the roads is continuously increasingat an alarming rate around the world. This influences thedriving conditions and could create harsh and even hazardousdriving conditions. Particularly, the number of accidents iscontinuously increasing which results in physical damagesand victims. Drivers are also encountering increasing difficultiesto reach their destinations because of intense congestions.As a result, there is a great need for drivers to be

assisted bycontrol systems and assistance applications to enhance theirsafety on the road particularly when urgent events occur suchas accidents, congestions, bad weather conditions, etc. Theautomotive industry and academic researchers are movingtowards inter-vehicles communications-based services providedwithin the context of vehicular ad-hoc networks regularlycalled VANETs [1]. In VANETs, vehicles will cooperateamong themselves to benefit from a wide range of applications[2]. Nevertheless the open architecture of vehicularenvironment inevitably makes it vulnerable to many securityissues. This forces vehicles to be careful about their cooperationwith other peers. Vehicles exchange short messages(generally called alerts [1]) about occurring urgent eventson the road. They have then to authenticate not only thenode transmitter of such messages but also the receivedinformation since a legitimate node might relay a fraudulentinformation. For instance, a malicious vehicle mightmodify information about a real event such as the position, thetime of occurrence, etc, or it might create fraudulent eventswhich are not real in order to disturb other drivers behavior[3]. Recently, trust models are proposed as an emergingtechnique allowing the establishment of the minimal securitylevel between cooperative nodes [4][6]. Trust computingsystems target the information itself, they allow checkingdata reliability. Trust systems provide other network securityservices such as access control, authentication, maliciousvehicles detection and secure resources sharing [4], [7], [8].Consequently, it is important to periodically evaluate thetrustworthiness of vehicles using some metrics and computationalmethods.There exists two main categories of trust computing protocols:infrastructure-based and self-organized [4]. In theinfrastructure-based approach, all vehicles relate to a trustedauthority that provides certificates or static trust valuesto vehicles to be authenticated. In fact, possessingwork.However, in VANETs the authentication is insufficientto decide about the trustworthiness of the vehicles because itdoes not target the reliability of messages. Besides, vehiclesare traveling for long distances, and they are continuouslyconfronted with other unknown vehicles that can be registeredwith other certification authorities in other regions.As such, infrastructure-based trust models may not be sufficient in VANETs. Regarding the self-organized trust establishmentmodels, the trustworthiness of vehicles is builtand maintained in a distributed fashion [9], [10]. Indeed,each vehicle collects information from unknown vehiclesin its neighborhood along short periods of time. The trustrelationship in distributed systems can be established eitherdirectly based on mutual communications between vehiclesor indirectly based

on relayed information about other remotevehicles, or by combining both. In the latter, the generalprinciple is to check many criteria related to the data messagesexchanged between the vehicles in the context of e-Safetyapplications and the context of generation of these messagessuch as the position of the transmitter, the freshness of themessage [11], and the role of the transmitter vehicle in thenetwork (usual vehicle, police, emergency vehicle, etc.) [12].

Nevertheless, these meta-data used in the majority of proposalsare not sufficient to decide on the trustworthiness ofthe data and the vehicle itself. In fact, a malicious vehiclelocated in the event zone might alter correspondence messagesor create fake urgent events. Furthermore, the majorityof existing self-organized proposals are based on recommendationsfrom other vehicles or from the road side units about agiven vehicle [13]. However, the additional traffic generatedby the recommendation requests/responses might slow downapplications such as e-Safety.In order to circumvent these shortcomings, we proposea new fully distributed trust computing framework aimingto continually evaluate the trustworthiness of vehicles andprovide a reliable data transmission process. The groundprincipal of our protocol, termed Enhanced Distributed TrustComputing Protocol EDCTP, is that each vehicle checks thereliability of the alerts messages received from its neighbors,and maintains a trust metric reflecting the credibility of eachtransmitter over time. We previously proposed in [14], a firstvariant of EDTCP where all vehicles reaching a trust metricvalue equal to 0 are deemed malicious vehicles, and consequentlyare definitely excluded from the network.

Our contribution in this paper is threefold. First, we proposea newtier-based approach to disseminate Alert messagesin VANETs. The aim is to mitigate malicious behavior in thenetwork and to recognize fake events which are announcedby malicious vehicles before moving away from the sourceof the event. Secondly, we propose an enhanced distributedtrust computing protocol aiming to assign trust levels to vehiclesthat contributed in the dissemination of alert messages.We aim to detect the largest set of fully trusted vehicles aswell as all malicious vehicles without excluding them fromthe network as in DTCP [14]. Our proposed EDTCP is onlybased on the inspection of the direct experience betweennodes without using of any recommendation system. Ourthird contribution concerns the analytical modeling using atime dependent birth-death process to investigate the efficiency of EDTCP in computing the trust

metrics of maliciousvehicles.The paper is organized as follows. In section II, we summarizethe relevant related work. In section III, we present theproposed protocol as well as the analytical modeling of thetrust metric time evolution of malicious nodes. In section IV,we present the performance evaluation of our proposedframework. Section V concludes the paper and presents somefuture orientations.

RELATED WORKS

We first expose relevant research proposals related to datadissemination in VANETs. Then we will present some ofthe relevant research work related to trust establishment invehicular environments.

A. DATA DISSEMINATION IN VANETs

Many solutions targeting data dissemination in Vehicularnetworks have been proposed [15][17].In [18], a traffic information propagation approach isproposed. Traffic is sent through two channels. A receiververifies the message integrity by checking if messagesreceived from both channels match correctly. In the proposedapproach, vehicles in each direction of a two-way road forma separated media channel to forward messages. As such, agenerated message has two separated and independent mediachannels to be propagated. In order to accept a message,a recipient vehicle must receive two identical messages fromboth directional channels to be sure that the message has notbeen altered. This approach is however only efficient in anurban scenario as it needs a rather high vehicle density.In [19], the authors dealt with the position cheating attackin the FMBA protocol [20]. In particular, the goal of thisattack is to induce a delay in the broadcast of the alertmessages by increasing the Contention Window of honestvehicles. They proposed a secure inter-vehicular protocol todisseminate accident warnings, resilient against the positioncheating attack. In [21], the authors proposed a newcombinedarchitecture of V2V communication, delay tolerant networkand V2I communication for large scale data disseminationin VANETs.

The aim is to compensate disconnections andnetwork partitioning. A hybrid approach on message propagationis proposed in [22] for low density vehicular networks.In [23], Palazzi et al. proposed a novel inter-vehiclescommunication architecture that adapts its functionalities toserve

applications by quickly propagating their messagesthroughout a vehicular network. Particularly, a priorityscheme is proposed in order to choose the next-hop forwarderof a broadcast message based on the distance from theprevious sender and the expected transmission range. Theyaimed to reduce redundant transmissions. In order to achievea fast multi-hop broadcast of a message, the farthest vehicle within the transmission range is always chosen to be the nextforwarder. A smart broadcast protocol is proposed in [24]where to each received message corresponds a receiving areadivided into a set of non overlapping and adjacent sectors.

To each sector corresponds a contention windows. Uponreceiving a message, a vehicle determines the sector to whichit belongs.We note here that in all the above cited research efforts,authors tried to minimize message redundancy and data traffic, however they did not target the reliability and the authenticityof the broadcast information. In fact, the quality ofinformation is a requirement in the context of vehicular networkswhere meta-data can be used to provide an assessmentof the reliability of collected data. In this respect, attentionshould be paid to the trust properties like security, reliability,as well as data collection efficiency. In our novel framework,we proposed a new data dissemination technique where thereliability of occurring events and the authenticity of correspondenttransmitted data messages are checked.

B. TRUST MANAGEMENT IN VANETS

Trust establishment is a fundamental issue in vehicular ad hocnetworks since smart devices embedded on vehicles have toprocess and handle the data in compliance with user needsand rights. Trust provides an effective way to evaluate credibilitybetween vehicles and to assist them to make a wisedecision to communicate and collaborate with each other.In vehicular ad hoc networks, a trust model must be scalableproviding the same performances independently of the size and the density of the network. The rapid change ofthe road conditions remains one of the issues and challengesfacing trust establishment in VANETs. Exchangedinformation needs to be evaluated according to its particularcontext [9], [12]. In addition, a vehicle must be ableto trust the received information in a reasonable shorttime [3], [4], [25], [26].In [27], Tajeddine et al. proposed an approach to preservethe privacy of users in their proposed reputation-basedtrust model. To this end, vehicles are organized off-line intogroups. Each group has a manager, a unique identifier and aunique signature.

Additionally, each group has a reputationvalue. When a vehicle v receives messages reporting theroad state from one or more vehicles belonging to the samegroup s(gv), it first calculates an average of all road statesS(gv). Then, v calculates the total road state TS combiningall the road states received from all groups. After decidingabout the real state of the road using TS, vehicle v updatesthe group reputation value by comparing S(gv) to the TS.If S(gv) is equal to TS, the group reputation will be increasedotherwise it will be decreased. In this approach, the reputationof the group is correlated with the behavior of each member.

As such, the approach is not resilient against a collusionattack when a set of vehicles belonging to a given groupbroadcast false information using the credentials of the samegroup. The authors did not describe any technique aboutforming the groups on the road, yet another shortcoming of this approach is the absence of trust values for the vehicles inorder to punish malicious ones.In [28], the authors proposed a fuzzy approach to decidewhether to accept a warning message from other vehiclesbased on the trustworthiness of the issuer. To this end, vehiclesare classified according to their calculated reputationscores into three categories represented by fuzzy sets. First,each vehicle v computes a trust score for each other vehicle j.It takes into account recommendations from other vehiclesabout vehicle j, the old reputation score that v holds on j andthe recommendations about vehicle j from eventual road sideunits (RSUs). Then, vehicle v projects the reputation score ofj on one of the fuzzy sets and according to the set to whichvehicle j belongs to, vehicle v decides about trusting theinformation received from j. In this model, authors assumedthat vehicle v requests its neighbors about the reputation ofvehicle j which might cause supplementary network traffic.

Furthermore, both sending recommendation requests to andreceiving responses from RSUs need additional time. In addition,the proposed approach can discard a high number ofcorrect messages.The authors in [29] proposed a data-based trust model forephemeral networks. First, each vehicle computes a reportabout an event by combining two types of information: staticinformation such as the type of vehicle and the event type anddynamically changing information such as the security stateof the vehicle and its location. Then all those trustworthinessreports about the same event are combined and their validity isinferred by a decision module using an evaluation techniquesuch as weighted voting and Bayesian Inference

to decideif the reported event really occurred. Using this model, onlytrust on data is checked, however the trust between vehiclesis not established.

In [30] it has been proposed to classify vehicles encounteringthe same traffic event into different roles in order todetermine whether the received information is trustworthy.In fact, when a vehicle receives a traffic message from anevent reporter, it observes whether the behavior of the reportercorresponds to the standard behavior. In the affirmative, thevehicle accepts the message and calculates its reputationvalue by combining the role of the reporter and the reputationvalues of the received event from other vehicles using a fuzzyapproach. We notice that this solution is not realistic sinceauthors relied on the behavior of the vehicle reporter of theevent to decide about a trafc message.

In [31], Dotzer et al. proposed a hybrid approach using apiggybacking technique. In their proposal, a trustworthinessopinion is appended to each message reporting an event. Thedrawback of this proposal is that the first opinion appendedto the message affects other opinions because its computingis recursive. It is based on the opinion received in themessage. In [32], the authors considered a subset of trustedvehicles in the network called anchors. They assumed thatthe anchors broadcast only reliable messages. The data validationis ensured either by comparing the received datawith other vehicles agreement or with the data received from the anchors. The validation process is only accurate when ahigh number of reports is received from other vehicles.

Shaik and Alzaharani proposed in [11] a new approachaiming to alter out malicious vehicles. It is based on thedetection of false location and time information. The schemeconsists of three interrelated steps. First a vehicle calculatesa confidence value for each data message received from itsneighbors. This confidence value is computed as a functionof the location closeness of the vehicle to the event locationand the time received in the data message compared to theinstant of the event occurrence. Then, a trust value for eachmessage is computed based on the confidence value. Thistrust value is used to decide about the forwarding of themessage. However, the location and the time verification areonly accurate if the receiver receives the signal directly fromthe sender otherwise the false positive rate gets too high.

In [12], the authors proposed a data centric approach basedalso on the location closeness of the reporter to the event andthe freshness of the data. However, the location metric is notsufficient to decide about the legitimacy of the transmitteddata and the trustworthiness of the transmitter as the messagemay emanate from a malicious vehicle located near the event.In [33] and [34], proposals are based on the Dempster-Shafer theorem (DST) [35]. DST is used in order to combinemany independent beliefs about a given vehicle in orderto compute the trust metrics.

The shortcoming of such anapproach is due to old beliefs received from other nodes.Furthermore, erroneous trust beliefs about a vehicle mightinduce an erroneous computed trust metric.Trust is also used in designing secure routing protocols[36], [37]. In [38], the authors proposed TROUVE whichis a trust based routing protocol for vehicular networks.Each node stores information about its neighbors includingthe Packet Drop Ratio (PDR) and Packet Sent Ratio (PSR).In order to compute the trust metric, each vehicle comparesthe PDR and the PSR to a given threshold and updates thetrust metric accordingly.

In this paper, we propose an Enhanced and DistributedTrust Computing Protocol (EDTCP) to compute and maintainthe trust levels. Our protocol is fully distributed where eachvehicle evaluates the trust level of its 1-hop neighbors fromwhich it receives alert messages without using any internalor external recommendations. Trust evaluation is based onthe assessment of the authenticity of transmitted messages.To this end, we propose a new data dissemination techniqueaiming to alter out non authentic events and to mitigatethe impact of falsified data transmitted by malicious nodes.Each node evaluates the authenticity of announced eventstransmitted by its neighbors and updates their trust levels overthe time according to its observations.

RESEARCH ISSUES AND OPPORTUNITIES

First, we describe the new tier-based alerts dissemination technique. Then, we present our newtrust computing protocoland the analytical modeling of the trust metric of malicious vehicles. The purpose of vehicular networks is to equip vehicles with the capability of communication and to provide many services aiming to assist drivers and to enhance their safety

on the road. Those services provide information to drivers regarding meteorological conditions, obstacles, accidents, traffic jam, etc. Information are received from the neighbors of the vehicle or from sensors embedded on the vehicle itself. In fact, vehicles exchange data messages, conventionally called alerts [39], about their surrounding in order to share their observations and inform remote vehicles about occurring events on the road. Furthermore, the transmission of alert messages is periodic and their size is reduced. Conventionally, an alert message contains a description of the occurring event such as position, instant of occurrence, intensity of caused damage, etc [2], [40]. However, some malicious vehicles may claim harmful non-existent events, and broadcast fake messages in order to create certain situations on the roads. For example, a malicious vehicle for its own purpose sends fake messages in order to inform other vehicles about non-existent traffic jam, accident, or closed road. This malicious behavior is regularly called bogus information attack

CONCLUSION

In this paper, we proposed a new trust computing protocolcalled EDTCP for VANETs. The aim is to monitorvehicles behavior in order to detect the largest set offully trusted vehicles. Furthermore, we proposed a new datadissemination technique based on tiers in order to mitigate the impact of vehicles misbehavior, and detect virtually allmalicious vehicles. In the proposed framework, each vehiclechecks the authenticity of the messages received from itsneighborhood, and then assigns to the transmitter a trustmetric. This trust metric is continuously updated dependingon the authenticity of the received messages. We modeledthe evolution of the trust metric of malicious vehicles usinga time dependent M=M=1=N process. Extensive simulations were performed to show the validity of the proposed modeland to evaluate the efficiency of EDTCP. Other aspects ofmisbehavior are being considered as an extension to ourproposed framework.

References

[1] IEEE Standard for Information TechnologyTelecommunications andInformation Exchange Between SystemsLocal and Metropolitan AreaNetworksSpecific Requirements Part 11: Wireless LAN Medium AccessControl (MAC) and Physical Layer (PHY) Specifications Amendment6: Wireless Access in Vehicular Environments, IEEE Standard 802.11,Nov. 2005.

[2] E. C. Eze, S.-J.Zhang, E.-J. Liu, and J. C. Eze, ``Advances in vehicularad-hoc networks (VANETs): Challenges and road-map for future development,"Int. J. Auto. Comput., vol. 13, no. 1, pp. 118, 2016.

[3] B. Mokhtar and M. Azab, ``Survey on security issues in vehicular adhoc networks," Alexandria Eng. J., vol. 54, no. 4, pp. 11151126, 2015,doi: 10.1016/j.aej.2015.07.011.

[4] K. Govindan and P. Mohapatra, ``Trust computations and trust dynamicsin mobile adhoc networks: A survey," IEEE Commun. Surveys Tuts.,vol. 14, no. 2, pp. 279298, 2nd Quart., 2012, doi: 10.1109/SURV.2011.042711.00083.

[5] Z. Yan, P. Zhang, and A. V. Vasilakos, ``A survey on trust managementfor Internet of Things," J. Netw. Comput. Appl., vol. 42, pp. 120134,Jun. 2014.

[6] S. A. Soleymani et al., ``Trust management in vehicular ad hoc network:A systematic review," EURASIP J. Wireless Commun. Netw., vol. 2015,no. 1, p. 146, Dec. 2015.

[7] N. Karthik and V. S. Ananthanarayana, ``A hybrid trust managementscheme for wireless sensor networks," Wireless Pers. Commun., vol. 97,no. 4, pp. 51375170, Dec. 2017.

[8] S. Goli-Bidgoli and N. Movahhedinia, ``Determining vehicles' radiotransmission range for increasing cognitive radio VANET (CR-VANET)reliability using a trust management system," Comput. Netw., vol. 127,pp. 340351, Nov. 2017.

[9] P. Agarwal and N. Bhardwaj, ``A review on trust model in vehicular ad hocnetwork," Int. J. Grid Distrib.Comput., vol. 9, no. 4, pp. 325334, 2016.

[10] U. Khan, S. Agrawal, and S. Silakari, ``Detection of malicious nodes(DMN) in vehicular ad-hoc networks," Proc. Comput. Sci., vol. 46,pp. 965972, Jan. 2015.

[11] R. A. Shaikh and A. S. Alzahrani, ``Intrusion-aware trust model for vehicularad hoc networks," Secur. Commun.Netw., vol. 7, no. 11, pp. 16521669,2014.

[12] X. Yao, X. Zhang, H. Ning, and P. Li, ``Using trust model to ensurereliable data acquisition in VANETs," Ad Hoc Netw., vol. 55, pp. 107118,Feb. 2017.

[13] C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano, and P. Manzoni,``T-VNets: A novel trust architecture for vehicular networks using the standardizedmessaging services of ETSI ITS," Comput. Commun., vol. 93,pp. 6883, Dec. 2016.

[14] T. Gazdar, A. Belghith, and A. AlMogren, ``DTCF: A distributed trustcomputing framework for vehicular ad hoc networks," KSII Trans. InternetInf. Syst., vol. 11, no. 3, pp. 15331556, 2017.

[15] N. Kaur and A. Singh, ``A survey on data dissemination protocols used inVANETs," Int. J. Comput. Appl., vol. 120, no. 23, pp. 4350, Jun. 2015.

[16] X. Li and H. Li, ``A survey on data dissemination in VANETs," Chin. Sci.Bull., vol. 59, no. 32, pp. 41904200, 2014.

[17] R. S. Schwartz, H. Scholten, and P. Havinga, ``A scalable data disseminationprotocol for both highway and urban vehicular environments,"EURASIP J. Wireless Commun.Netw., vol. 2013, no. 1, p. 257, 2013.

[18] B. Aslam, S. Park, C. C. Zou, and D. Turgut, ``Secure traffic data propagationin vehicular ad hoc networks," Int. J. Ad Hoc Ubiquitous Comput.,vol. 6, no. 1, pp. 2439, 2010.

[19] W. B. Jaballah, M. Conti, M. Mosbah, and C. E. Palazzi, ``A secure alertmessaging system for safe driving," Comput.Commun., vol. 46, pp. 2942,Jun. 2014.

[20] C. E. Palazzi, S. Ferretti, M. Roccetti, G. Pau, and M. Gerla, ``How do youquickly choreograph inter-vehicular communications? A fast vehicle-tovehiclemulti-hop broadcast algorithm, explained," in Proc. IEEE CCNC,Jan. 2007, pp. 960964.

[21] K. Paridel, J. Balen, Y. Berbers, and G. Martinovi¢, ``VVID: A delay tolerantdata dissemination architecture for VANETs using V2V and V2I communication,"in Proc. 2nd Int. Conf. Mobile Serv., Resour., Users (MOBIL-ITY), 2012, pp. 16.

[22] A. M. Vegni and T. D. C. Little, ``A message propagation model forhybrid vehicular communication protocols," in Proc. 7th Int. Int. Symp.Workshop Commun. Technol. Veh. Syst. Netw. Digit. Signal Process.,Newcastle Upon Tyne, U.K., Jul. 2010, pp. 382386.

[23] C. E. Palazzi, M. Roccetti, and S. Ferretti, ``Anintervehicular communicationarchitecture for safety and entertainment," IEEE Trans. Intell. Transp.Syst., vol. 11, no. 1, pp. 9099, Mar. 2010.

[24] E. Fasolo, R. Furiato, and A. Zanella, ``Smart broadcast algorithm forinter vehicular communications," in Proc. WPMC, Aalborg, Denmark,Sep. 2005, pp. 15831587.

[25] J. Zhang, ``A survey on trust management for VANETs," in Proc. 25thIEEE Int. Conf. Adv. Inf. Netw. Appl. (AINA), Singapore, Mar. 2011,pp. 105112.

[26] Q. Alriyami, A. Adnane, and A. K. Smith, ``Evaluation criterias for trustmanagement in vehicular ad-hoc networks (VANETs)," in Proc. Int. Conf.Connected Veh. Expo (ICCVE), Vienna, Austria, 2014, pp. 118123.

[27] A. Tajeddine, A. Kayssi, and A. Chehab, ``A privacy-preserving trustmodel for VANETs," in Proc. Int. Conf. Comput. Inf. Technol., 2010,pp. 832837.

[28] F. G. Mármol and G. M. Pérez, ``TRIP, a trust and reputation infrastructurebasedproposal for vehicular ad hoc networks," J. Netw. Comput. Appl.,vol. 35, no. 3, pp. 934941, May 2012.

[29] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P.Hubaux, ``Ondatacentrictrust establishment in ephemeral ad hoc networks," in Proc. IEEEINFOCOM, Phoenix, AZ, USA, Apr. 2008, pp. 19.

[30] Q. Ding, X. Li, M. Jiang, and X. Zhou, ``Reputation-based trust model invehicular ad hoc networks," in Proc. Int. Conf. Wireless Commun. SignalProcess., Suzhou, China, 2010, pp. 16.

[31] F. Dotzer, L. Fischer, and P. Magiera, ``VARS: A vehicle Ad-hoc networkreputation system," in Proc. 6th IEEE Int. Symp. World Wireless MobileMultimedia Netw. (WoWMoM), Taormina-Giardini Naxos, Italy, 2005,pp. 454456.

[32] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, ``A data intensive reputationmanagement scheme for vehicular ad hoc networks," in Proc. 3rdAnnu. Int. Conf. Mobile Ubiquitous Syst.-Workshops (MOBIQUITOUS),San Jose, CA, USA, Jul. 2006, pp. 18.

[33] Z. Wei, F. R. Yu, and A. Boukerche, ``Trust based security enhancementsfor vehicular ad hocnetworks," in Proc. 4th ACM Int. Symp. Develop.Anal.Intell.Veh.Netw. Appl. (DIVANet), Montreal, QC, Canada, 2014,pp. 103109, doi: 10.1145/2656346.2656353.

[34] K. Sharma and B. K. Chaurasia, ``Trust based location finding mechanismin VANET using DST," in Proc. 5th Int. Conf. Commun. Syst. Netw.Technol., Gwalior, India, 2015, pp. 763766.

[35] L. A. Zadeh, ``A simple view of the Dempster-Shafer theory of evidenceand its implication for the rule of combination," AI Mag. J., vol. 7, no. 2,pp. 8590, Jul. 1986.

[36] K. Dixit, K. K. Joshi, and N. Joshi, ``Anovel approach of trust based routingto select trusted location in AODV based VANET: A survey," Int. J. HybridInf. Technol., vol. 8, no. 7, pp. 335344, 2015.

[37] N. J. Patel and R. H. Jhaveri, ``Trust based approaches for secure routing inVANET: A survey," Proc. Comput. Sci., vol. 45, pp. 592601, Jan. 2015.

[38] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, ``TROUVE:A trusted routing protocol for urban vehicular environments," in Proc.IEEE 11th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob),Oct. 2015, pp. 260267.

[39] M. L. Sichitiu and M. Kihl, ``Inter-vehicle communication systems:A survey," IEEE Commun. Surveys Tuts., vol. 10, no. 2, pp. 88105,2nd Quart., 2008.

[40] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, ``A comprehensivesurvey on vehicular ad hoc network," J. Netw.Comput. Appl.,vol. 37, pp. 380392, Jun. 2014.

[41] B. Lipi«ski, W. Mazurczyk, K. Szczypiorski, and P. ‘ mietanka, ``Towardseffective security framework for vehicular ad-hoc networks," J. Adv. Com-put. Netw., vol. 3, no. 2, pp. 134140, 2015.

[42] T. Gazdar, A. Benslimane, A. Belghith, and A. Rachedi, ``A secure clusterbasedarchitecture for certificates management in vehicular networks,"Secure. Commun.Netw., vol. 7, no. 3, pp. 665683, 2014.

[43] A. M. K. Tarabia, ``Transient analysis of M/M/1/N queueAn alternativeapproach," Tamkang J. Sci. Eng., vol. 3, no. 4, pp. 263266, 2000.

[44] L. Kleinrock, Queueing Systems: Theory, vol. 1. Toronto, ON, Canada:Wiley-Interscience, 1975.

[45] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, ``SUMOSimulation of urban mobility: An overview," in Proc. 3rd Int. Conf. Adv.Syst. Simulation (SIMUL), Barcelona, Spain, Oct. 2011, pp. 6368.

[46] A. Varga, ``The OMNeTCC discrete event simulation system," in Proc.Eur. Simulation Multiconf. (ESM), Jun. 2001.