# A Review on VANET And Reputation Scenario

**Mithun Sahay[1], Anand Singh Bisen[2]**
[1, 2] Department of Computer Science
[1, 2] VITM, Indore, India

***Abstract***- *Vehicular communication is a significant and evolving field of research in the area of vehicular technology. The evolution of software and hardware in communication systems assists to the generation of new networks. VANETs are sort of the ad hoc networks real-life applications, where vehicles communicate among each other and with set components termed as roadside units. VANETs have their distinctive characteristics and necessities that vary from those in regular ad-hoc networks, but the security remains a foremost challenge since of the dynamic topology and the deficient of infrastructure. In this paper we present a survey on Trust and Reputation model in VANET, their also present challenges and application in VANET and study of various researcher work in VANET reputation.*

***Keywords***- VANET; Trust; Repudiation; Hidden Markov Model

## I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) have turned into an important research area over the last few years. VANETs are distinguished from MANET by their hybrid network architectures, node movement characteristics, and new application scenarios. VANETs [1, 2] perform crucial functions in road safety, such as detection of traffic accidents and reduction of traffic congestions. By exchanging real-time warning messages through vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication, VANETs present the capability of providing local information in near-real time to enhance the safety of drivers and improve mobility. Reputation and trust are two essentials tools of security that are used to facilitate decision making in VANETs. In general, reputation is the opinion of one entity as vehicles in VANETs about another [3]. Essentially it signifies the trustworthiness of a vehicle in VANETs. Trust in general is the level of confidence in a person or a thing [4]. In VANETs, it is the expectation of one vehicle about the action of another vehicle [5].

### Characteristics of VANETs

Drive behavior, constraints on mobility, and high speeds create unique Characteristics in VANETs. These characteristics distinguish them from other mobile ad hoc networks, and the major characteristics are as follows:

1. **High mobility and Rapid changing topology:** Vehicles move very fast especially on highways. Thus, they stay in the communication range of each other just for several seconds, and links are established and broken fast. When the vehicle density is low or existing routes break before constructing new routes, it has higher probability that the vehicular networks are disconnected. So, the previous routing protocols in MANET are not suitable for VANETs.

2. **Geographic position available:** Vehicles can be equipped with accurate positioning systems integrated by electronic maps. For example, GPS receivers are very popular in cars which help to provide location information for routing purposes.

3. **Mobility modeling and predication:** Vehicular nodes are usually constrained by prebuilt highways, roads and streets, so given the speed and the street map, the future position of the vehicle can be predicated. Vehicles move Malong pre-defined paths, this provides an opportunity to predict how long routes would last compared to arbitrary motion patterns like the random waypoint model [6].

4. **Hard delay constraints:** In VANETs applications, such as the collision warning or Pre-Crash Sensing, the network does not require high data rates but has hard delay constraints, and the maximum delay will be crucial.

5. **No power constraint:** Since nodes are cars instead of small handheld devices, power constraint can be neglected thanks to always recharging batteries.

### Challenges of VANET

### 1. Mobility

The basic idea from Ad Hoc Networks is that each node in the network is mobile, and can move from one place to another within the coverage area, but still the mobility is limited, in Vehicular Ad Hoc Networks nodes moving in high mobility, vehicles make connection throw their way with another vehicles that maybe never faced before, and this connection lasts for only few seconds as each vehicle goes in its direction, and these two vehicles may never meet again. So securing mobility challenge is hard problem [8].

2. **Volatility**

The connectivity along with nodes can be extremely ephemeral, and maybe will not happen again, vehicles travelling throw coverage area and making connection with other vehicles, these connections will be lost as each car has a high mobility, and maybe will travel in opposite direction[7][8]. This network lacks the relatively long life context, so personal contact of user's device to a hot spot will require long life password and this will be impractical for securing VC [9].

3. **Privacy VS Liability**

Liability provides a better opportunity for legal analysis and denial of such information is impossible (in case of accidents) [7], other than the privacy mustn't be violated [9].

4. **Network Scalability**

With the increase in the percentage of vehicles in the world, scalability of the network is becoming challenging. The network should be scalable such that if more number of nodes or cars is added, it should function in proper manner [9].

**Security requirements of VANET**

VANET must fulfill some security prerequisites before they are transferred. A security system in VANET should fulfill the following necessary condition [10]:

a) **Authentication:**

Authentication guarantees that the message is produced by the honest to legitimate client. In VANET a vehicle responds upon the information originated from the other vehicle consequently authentication must be fulfilled.

b) **Availability:**

Availability obliges that the data must be accessible to the real clients. DOS Attacks can cut down the network and hence information can't be shared.

c) **Non-Repudiation:**

Non-repudiation implies a node can't deny that he/she doesn't transmit the message. It might be pivotal to focus the right arrangement in accident reproduction.

d) **Privacy:**

The privacy of a node against the unauthorized node should be ensured. This is obliged to eliminate the message delay attack.

e) **Data Verification:**

A generally confirmation of data is obliged to take out the false messaging.

## II. TRUST IN VANET

Trust is the key element in creating a trusted vehicular environment which promotes security in vehicular networks. Trust is either in human behavior or in the deployed hardware both forming a trusted communication environment. Few trust models had been introduced to enforce honest information sharing between communicating nodes [11], [12].

## III. REPUDIATION IN VANET

In VANET, a significant problem is that how to trust the particular vehicle or message. For example, if a car forwards the message that there is jamming at location X, be supposed to other vehicles suppose this car as well as this message and then make a corresponding action? Researchers come up with the method which called reputation system to solve this issue.

In ad hoc networks, nodes are both terminals and routers for the lack of routing infrastructure; they have to cooperate with each to exchange information. Misbehavior means deviation from regular action; node could misbehave for selfish reasons and consequently impact the system. The goal of reputation system is to establish trust value for every node in this network, and depending on these values, the other nodes make a decision whom to trust consequently promote reliable activities. Resnick and Zeckhauser [13] list three aims for reputation systems:

1. To provide data to differentiate among a truthful peer and an unreliable peer.
2. To support peers to operate in a truthful way.
3. To depress unreliable peers from taking part in the service, the reputation mechanism is offered.

**Repudiation Models**

### A. Role Definition

First, depending on the different role vehicles played encounter the same traffic event, we categorize them as shown in fig.1.

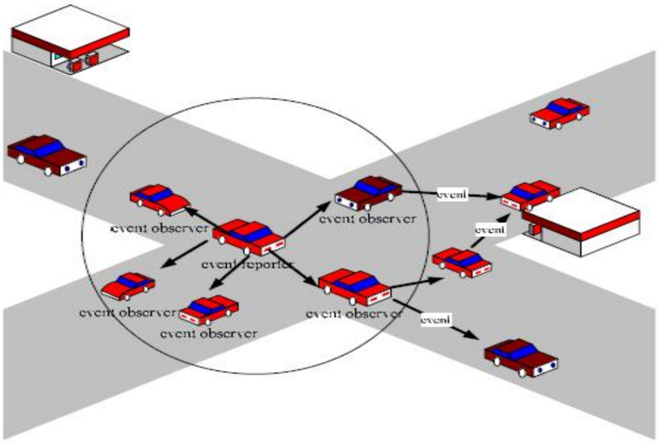

Fig.1: Categorize Member

#### a) Event Reporter (ER):

We call a vehicle an event reporter, if it can perceive incident by equipped sensors, then send alarm messages to other neighboring vehicles.

#### b) Event Observer (EO):

Within one hop of an event reporter, vehicles are capable of sensing the action of event reporter after reception of event message from it. We call these vehicles event observers.

#### c) Event Participant (EP):

We call other vehicles beyond one hop of an event reporter as event participants, as they can take delivery of and transmit the event message, but it is unfeasible to recognize the actions of event reporter.

### B. Event Propagation

In our model, traffic information comes both from expected messages by means of wireless interface and on-board sensors. Every vehicle has an event table that records all arrived and consequent traffic event information, namely event ID, event type, episode timestamp, event position, communication range, and event reputation value. In the event table, every record entry maintains a distinctive traffic event. A sensor can sense the equivalent event several times after a traffic event takes place, then these detect event messages are assigned a unique ID.

When an ER encounters a traffic event, traffic-associated information will be gathered by sensors in this vehicle. Relaying on the sense frequency, ER can calculate the harshness of this traffic event and set the reputation value of it. If this value is over the specified threshold, the event message will be transmitted to the traffic safety application in the vehicle and to all neighbors in one hop, namely EO.

In our design, EO is a very important role to identify bogus event messages. When an EO gets traffic warning message from an ER, firstly it records this message into the event table if there exist no the identical identities record in the table. Within Δtime, this EO can receive the event message with this ID n times from this ER. By observing succeeding behavior of ER in this phase, an EO can estimate the truthfulness of this event message though it does not encounter the event directly. Intuitively, if the behavior of ER matches the typical behavior model related to the traffic event type, the event message is considered as trusty. For example, when an ER sends an “obstacle” type event message, the “correct” corresponding driver behavior should be “decelerate” or “change lane”. So if an EO found other behaviors of an ER except standard behavior model, it is reasonable to confer that this event message from the ER maybe bogus. Then the reputation value of this event message is set to low by this EO. At the same time, this EO maybe receive many event messages with this ID from other ERs, EOs and EPs, we give a complex formula to integrate all these second-hand information in next section.

For an EP, it only can receive messages from Eos and other EPs. In next section, we also give a formula to calculate reputation value of event messages for EPs.

## IV. HIDDEN MARKOV MODEL

The Hidden Markov Model (HMM) is a stochastic model for sequential data. It is a stochastic process determined by the two interrelated mechanisms – a latent Markov chain having a finite number of states, and a set of observation probability distributions, each one associated with a state. At each discrete time instant, the process is assumed to be in a state, and an observation is generated by the probability distribution corresponding to the current state. The HMM is termed discrete if the output alphabet is finite, and continuous if the output alphabet is not necessarily finite, e.g., each state is governed by a parametric density function [14,15,16].

Theoretical and empirical results have shown that, given an adequate number of states and a sufficiently rich set of data, HMMs are capable of representing probability distributions corresponding to complex real-world phenomena in terms of simple and compact models [17,18]. This is supported by the success of HMMs in various practical applications, where it has become a predominant methodology for design of automatic speech recognition systems (ASR) [19,20,21]. It has also been successfully applied to various other fields, such as signature verification [22,23] communication and control [24,25], bioinformatics [26,27], computer vision [28,29], and computer and network security [30,31,32]. For instance, in the area of computer and network security, a growing number of HMM applications are found in intrusion detection systems (IDSs). HMMs have been applied either to anomaly detection, to model normal patterns of behavior, or in misuse detection, to model a predefined set of attacks. HMM applications in anomaly and misuse detection have emerged in both main categories of IDS - host-based IDS [32,33,30,31] and network-based IDS [33,34]. Moreover, HMMs have recently begun to emerge in wireless IDS applications [35,36].

In many practical applications, the collection and analysis of training data is expensive and time consuming. As a consequence, data for training an HMM is often limited in practice, and may over time no longer be representative of the underlying data distribution. However, the performance of a generative model like the HMM depends heavily on the availability of an adequate amount of representative training data to estimate its parameters, and in some cases its topology. In static environments, where the underlying data distribution remains fixed, designing a HMM with a limited number of training observations may significantly degrade performance. This is also the case when new information emerges in dynamically changing environments, where underlying data distribution varies or drifts in time. A HMM that is trained using data sampled from the environment will therefore incorporate some uncertainty with respect to the underlying data distribution [37].

It is common to acquire additional training data from the environment at some point in time after a pattern classification system has originally been trained and deployed for operations. Since limited training data is typically employed in practice, and underlying data distribution are susceptible to change, a system based on HMMs should allow for adaptation in response to new training data from the operational environment or other sources. The ability to efficiently adapt HMM parameters in response to newly-acquired training data, through incremental learning, is therefore an undisputed asset for sustaining a high level of performance. Indeed, refining a HMM to novelty encountered in the environment may reduce its uncertainty with respect to the underlying data distribution.

## V. RELATED WORK

Cao et al [38], extended the single-hop reputation announcement into a multi-hop version that enables carry-and-forward message propagation. In this scheme, we use Dempster Shafer theory to evaluate the reliability of messages and it guarantees better message flexibility and satisfactory message drop rate. The message utility rate and maximum message broadcasting bandwidth in multi-hop scheme cannot simultaneously dominate that of single-hop, because the maximal message broadcasting bandwidth always becomes large with the increase of message utility rate. However, this trade-off is up to vehicles to regulate based on their real needs. It is therefore more user friendly and flexible than single-hop. Moreover, the multi-hop scheme provides incentive for vehicles to participate in forwarding messages and at the same time maintains the robustness and privacy property of the single-hop scheme.

Izhak Rubinet.al in this paper [39] VANET networking schedule that is distinguished as a vehicular backbone network (VBN) through which vehicles that are found near legitimately chosen ostensible positions along a direct highway portion are chosen to serve as hand-off nodes. We utilize a stream affirmation control system at the source, controlling the pace of transmission of conceding bundles. Shut structure expository expressions are inferred for the rough reckoning of the framework's end-to-end throughput limit rate. Through recreation investigations, we affirm the accuracy of these explanatory figuring. We demonstrate the capacity of the framework to utilize vehicular CSMA/CA access plans too well copy the operations of the framework when overseen by the utilization of spatial-reuse TDMA plans. In planning the Heterogeneous system, we allocate system resource and dole out system parameters in a way that balances the throughput rates brought about over the cell remote access and VANET parts of the mixed network system.

K. S. Dhanalakshmi et.al [40], states the adoption of hybrid cryptographic methods for reducing the overhead on network, resolving major issues of Watchdog procedure. A novel key exchange approach termed as Instant Key Generation Mechanism (IKGM) is introduced here to eliminate the redistributed keys requirement. At this time the key encryption is performed at each node to enhance the performances next to existing techniques. It also provides highest malicious behavior detection rate which does not affect the significant performances of the network [40].

Afaf Bouhoute et.al [41], main objective of this paper is to show and learn driver conduct in the vicinity of diverse kind of traffic information. For this, we propose another formal way to deal with built a driving conduct, display that will be adjusted to an individual driver. To describe the model we characterize rectangular cross breed data yield automata formalism which comprises of an adjustment of an arrangement of ideas identified with the half breed automata idea. At that point, for model development, we propose an online uninvolved learning based way to deal with build the model as indicated by the watched driving conduct. The developed model may be valuable to anticipate the driver conduct later on, avert risky circumstances and give more comfort to the drive.

Alireza Marefat et.al [42], Presenting an intelligent driver assistant system in scenarios, performing the overwhelming move of a long vision discouraging Vehicle as a leader with a likelihood of another vehicle in front with snag probability out and about. The importance of this framework is to decrease the danger of using so as to overwhelm move in a mixture situation cases remote innovation taking into account Vehicular Ad hoc Network (VANET) to advance the driver's conduct in high hazard circumstances with direction for settling on a legitimate choice if there should be an occurrence of performing safe surpassing activity.

Zhiguang Cao et al [43], here two Calculations to assess the unwavering quality of messages and total the notoriety scores individually. The real rule of the unwavering quality assessment calculation is the Dumpster-Shafter Theory and the notoriety collection, calculation is a variation of weighted averaging capacity. To adjust the message scope region and the expense of sending messages, we additionally give a message sending standard. The proposed multi-bounce plan offers acceptable heartiness and jelly protection property. In particular, the multi-bounce plot ensures better message adaptability, as well as can create more tasteful message drop rate. What's more, in the message forward rule of our multi-bounce plan, it is up to the vehicles (i.e., Easy to understand) to manage the exchange off between the message utility rate and the maximal message telecasting bandwidth, based on their real needs.

Xiaoping Li et al [44], a Reputation-based Global Trust Establishment scheme (RGTEs). The plan acquaints an answer with offer the trust information in VANET securely by applying statistical laws, which makes it more utilized and exact to build up trust in quickly evolving environment. Additionally, we distinguish an awful node of the element edge as per constant notoriety status of the network. Analysis shows that RGTEs is more powerful in confidence-building, security affirmation and versatility.

Qin Li et al [45], described a novel declaration plan for VANETs in light of a notoriety system that permits assessment of message unwavering quality. We exhibit a protected and productive plan that is strong and shortcoming tolerant against the provisional inaccessibility of the central server.

## VI. CONCLUSION

In this paper we surveyed the fundamentals of VANET, its architecture, challenges, trust model and reputation model for VANET. Also present the literature of various works that has been done in VANET. For future work in VANET, we can calculate the trust on the basis of reply packet of other vehicles. Reputation builds by RSU on the basis of vehicle Reply packet and their behavior. Reputation calculates on the basis of **Hidden Markov model** and finding reputation score by Road Side Unit.

## REFERENCES

[1] J. Luo and J. P. Hubaux, "A survey of inter-vehicle communication," Tech. Rep. IC/2004/24, EPFL, Lausanne, Switzerland, 2004

[2] J. J. Blum, A. Eskandarian, and L. J. Huffman, "Challenges of intervehicle ad hoc networks," IEEE Transactions on Intelligent Transportation Systems, vol. 5, no. 4, pp. 347–351, 2004

[3] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey" IEEE Communications Surveys Tutorials Volume PP, Issue 99, **(2011)**, pp. 1-20.

[4] A. Tajeddine, A. Kayssi, A. Chehab, "A Privacy-Preserving Trust Model for VANETs," International Conference on Computer and Information Technology, **(2011)** China.

[5] H. Xu and D. W. Wen, "A trust-based routing protocol in ANET," In IJCSI International Journal of Computer Science Issues, vol. 10, Issue 1, no 2, **(2013)**, pp. 260-263.

[6] J. Broch, D.A Maltz, D.B. Johnson, Y-C Hu, and J. Jetcheva. "A Performance Comparison of Multi-Hop

Wireless Ad Hoc Network Routing Protocols," in Proc. of ACM/IEEE MOBICOM, 1998, pp. 85-97

[7] Surmukh Singh, Sunil Agrawal VANET Routing Protocols: Issues and Challenges Proceedings of 2014 RAECS UIET Panjab University Chandigarh, 06 08 March, 2014.

[8] Patrick I. Offor. Vehicle Ad Hoc Network (VANET): Safety Benefits and Security Challenges. Nova Southeastern University (po125@nova.edu). December 3, 2012.

[9] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures. Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET). National Advanced IPv6 Center, Universiti Sains Malaysia Penang, Malaysia. June 28, 2010.

[10] Maxim Raya e al., "The Security of Vehicular Ad Hoc Networks", SASN'05, Nov 7 2005, Alexandria, Verginia, USA, pp. 11-21

[11] J.Zhang, ―Trust management for VANETs: challenges,desired properties and future directions in International Journal of Distributed Systems and Technologies, pp.48-62, 2012

[12] J.Zhang, 2011,―A survey on trust management for VANETs in International Conference on Advanced Information Networking and Applications, pp.105-112

[13] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," Commun. ACM, vol. 43, no. 12, pp. 45–48, 2000.

[14] R.J. Elliott, Exact adaptive filters for Markov chains observed in gaussian noise, Automatica 30 (9) (1994) 1399–1408.

[15] Y. Ephraim, N. Merhav, Hidden Markov processes, IEEE Transactions on Information Theory 48 (6) (2002) 1518–1569.

[16] L. Rabiner, A tutorial on hidden Markov models and selected applications in speech recognition, Proceedings of the IEEE 77 (2) (1989) 257–286.

[17] Y. Bengio, Markovian models for sequential data, Neural Computing Surveys 2 (1999) 129–162.

[18] J.A. Bilmes, What HMMs can do. Tech. Rep. UWEETR-2002-0003, Dept of EE, University of Washington Seattle WA, 2002.

[19] L.R. Bahl, F. Jelinek, R.L. Mercer, A maximum likelihood approach to continuous speech recognition, IEEE Transactions on Pattern Analysis and Machine Intelligence, PAMI-5 2 (1982) 179–190.

[20] X. Huang, H.-W. Hon, Spoken Language Processing: A Guide to Theory, Algorithm, and System Development. Prentice Hall PTR, Upper Saddle River, NJ,USA, foreword By-Raj Reddy, 2001.

[21] O. Cappe, V. Buchoux, E. Moulines, Quasi-Newton method for maximum likelihood estimation of hidden Markov models, in: Proceedings of the 1998 IEEE International Conference onAcoustics, Speech, and Signal Processing, ICASSP98, vol. 4, 1998, pp. 2265–2268.

[22] A. El-Yacoubi, M. Gilloux, R. Sabourin, C. Suen, Unconstrained handwritten word recognition using hidden Markov models, IEEE Transactions on Pattern Analysis and Machine Intelligence 21 (8) (1999) 752–760.

[23] E. Justino, F. Bortolozzi, R. Sabourin, A comparison of SVM and HMM classifiers in the off-line signature verification, Pattern Recognition Letters 26 (9) (2005) 1377–1385.

[24] R.J. Elliott, Exact adaptive filters for Markov chains observed in gaussian noise, Automatica 30 (9) (1994) 1399–1408.

[25] G.E. Hovland, B.J. McCarragher, Hidden Markov models as a process monitor in robotic assembly, International Journal of Robotics Research 17 (2) (1998) 153–168.

[26] S.R. Eddy, Profile hidden Markov models, Bioinformatics 14 (9) (1998) 755–763.

[27] A. Krogh, B. Larsson, G. von Heijne, E.L.L. Sonnhammer, Predicting transmembrane protein topology with a hidden Markov model: application to complete genomes, Journal of Molecular Biology 305 (3) (2001) 567–580.

[28] M. Brand, V. Kettnaker, Discovery and segmentation of activities in video, IEEE Transactions on Pattern Analysis and Machine Intelligence 22 (8) (2000) 844–851.

[29] J. Rittscher, J. Kato, S. Joga, A. Blake, A probabilistic background model for tracking, in: Proceedings of the

6th European Conference on Computer Vision-Part II, ECCV00, Springer-Verlag, London, UK, 2000, pp. 336–350.

[30] S.-B. Cho, S.-J. Han, Two sophisticated techniques to improve HMM-Based intrusion detection systems, in: RAID, 2003, pp. 207–219.

[31] T. Lane, C.E. Brodley, An empirical study of two approaches to sequence learning for anomaly detection, Machine Learning 51 (1) (2003) 73–107.

[32] K. Lange, A quasi-Newton acceleration of the EM algorithm, Statistica Sinica 5 (1) (1995) 1–18.

[33] C. Warrender, S. Forrest, B. Pearlmutter, Detecting intrusions using system calls: alternative data models, in: Proceedings of the IEEE Computer

[34] Society Symposium on Research in Security and Privacy, Oakland, CA, USA, 1999, pp. 133–145.

[35] D.-Y. Yeung, Y. Ding, Host-based intrusion detection using dynamic and static behavioral models, Pattern Recognition 36 (1) (2003) 229–243.

[36] W. Khreich, E. Granger, A. Miri, R. Sabourin, Iterative Boolean combination of classifiers in the ROC space: an application to anomaly detection with HMMs, Pattern Recognition 43 (8) (2010) 2732–2752

[37] P. Domingos, A unified bias-variance decomposition and its applications, in: 17th International Conference on Machine Learning. Morgan Kaufmann, 2000, pp. 231–238.

[38] Zhiguang Cao, Qin Li , Hoon Wei Lim and Jie Zhang,” A Multi-hop Reputation Announcement Scheme for VANETs”. IEEE, 2014

[39] Izhak Rubin∗ , Yu-Yu Lin Andrea Baiocchi , Francesca Cuomo§ and Pierpaolo Salvo “Micro Base Station Aided Vehicular Ad Hoc Networking” 2014 International Conference on Computing, Networking and Communications, Invited Position Papers.

[40] K.S.Dhanalakshmi, Dr.B.Kannapiran, A.Divya “Enhancing Manet Security Using Hybrid Techniques in Key Generation Mechanism” 2014 International Conference on Electronics and Communication System (ICECS -2014)

[41] Afaf Bouhoute, Rachid Oucheikh, Ismail Berrada, Lahcen Omari “A New Formal Approach to Model Human Driving Behavior in Vehicular Networks” http://wits2014.science-conferences.net/.

[42] Alireza Marefat1 , Rozita Aboki2 , Ali Jalooli3 , Erfan Shaghaghi4 , Mohammad Reza Jabbarpour5 and Rafidah Md Noor6 “An Adaptive Overtaking Maneuver Assistant System Using VANET” APWiMob 2014, Bali 28-30 Augustus 2014

[43] Zhiguang Cao , Qin Li , Hoon Wei Lim and Jie Zhang “Multi-hop Reputation Announcement Scheme for VANETs” 978-1-4799-6058-3/14/$3l.00 ©2014 IEEE.

[44] Xiaoqing Li, Jicheng Liu, Xuejun Li and Weiying Sun “RGTE: A Reputation-based Global Trust Establishment in VANETs” 2013 5th International Conference on Intelligent Networking and Collaborative Systems

[45] Qin Li, Amizah Malip, Keith M. Martin, Siaw-Lynn Ng, and Jie Zhang “A Reputation-Based Announcement Scheme for VANETs” IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 9, NOVEMBER 2012.