International Journal of Digital Information and Wireless Communications (IJDIWC) 8(2): 139-143
The Society of Digital Information and Wireless Communications, 2018 ISSN: 2225-658X (Online); ISSN 2412-6551 (Print)

Trust Model for Group Leader Selection in VANET

Hamssa Hasrouny[1,2], Abed Ellatif Samhat[2], Carole Bassil[3], Anis Laouiti[1]
hamssa.hasrouny@telecom-sudparis.eu , samhat@ul.edu.lb , cbassil@ul.edu.lb , anis.laouiti@telecom-sudparis.eu
[1]Telecom SudParis, SAMOVAR, CNRS, University Paris-Saclay, 9 rue Charles Fourier - 91011 Evry Cedex, France
[2]Lebanese University, Faculty of Engineering-CRSI, Hadath Campus, Hadath, Lebanon
[3]Lebanese University, Faculty of Science II, Fanar Campus, Fanar, Lebanon

***Abstract*—In this paper, we propose a Trust Model for VANETs. It is a combination between centralized and distributed cooperation between vehicles and infrastructure to achieve the selection of the trustiest node as a Group Leader. The proposed model is based on different metrics to analyse the behaviour of the vehicles in the group while preserving the privacy of the participants and maintaining low network overhead. The evaluation of the proposed trust model is done by simulations using GrooveNet. Results show the efficiency of the proposed model to select the trusty vehicles.**

Keywords—Trust; Network Performance; Security Resistance; Decentralized.

I. INTRODUCTION

VANET (Vehicular Ad-hoc Network), a special class of mobile ad-hoc network with predefined routes, consists of vehicles capable of exchanging information by radio to improve road safety and/or to allow internet access for passengers. All vehicles are moving freely on road network communicating either with each other, or with RSU (Road Side Unit) and specific authorities. Using DSRC (Dedicated Short Range Communication) in a single or multi-hop, the communication mode is either V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure) or hybrid [1]. Securing exchanged messages between vehicles becomes a must.

After exploring the related work in the security architectures [2], standards [3], protocols, attacks, approaches and solutions in VANETs [4], many open issues and technical challenges in this field require investigation[1]. We investigate the ability of the network to self-organize via a high mobile network environment and we focus on the trustworthiness evaluation of nodes participating in VANET.

For the self-organisation we adopt the group formation approach where the Group Leader (GL) is the reference for all communications between its group members [5]. This lessens the periodic usage of RSU resources and minimizes the safety messages dissemination delay. But to select the trusty node as a Group Leader, we defined a Trust Model [6] to determine the trust metric of vehicles based on a modular secure architecture [7]. It involves a monitoring system processing based on cooperation of vehicles and validity of the broadcasted data. The trust metric in each node includes direct and indirect calculation based on many parameters. This metric when calculated is transmitted to the nearest GL which in turn overload all its trust metrics to the RSU. RSU as big data-center will merge and update these trust metrics and result a global trust metric for each node. The trust metric in its different stages has a threshold when exceeded the vehicle is considered trusty. The evaluation of the proposed trust model is done by simulations. Results show that this model is an efficient and reliable solution to elect potential GLs.

The rest of the paper is organized as follows: Section II presents some existing related works. Section III presents our proposed Trust Model. In section IV, we show the resistance of the proposed Trust Model against VANET security attacks. Simulation results evaluating the performance of our scheme are given in Section V. Finally, we conclude in section VI.

II. RELATED WORKS

Several works investigated the trust within VANET [8]- [23]. Various techniques are used to establish trust in the network: direct/indirect, centralized/distributed, proactive/reactive, data centric/attribute.

Trust establishment approaches can be divided into infrastructure based trust or self-organizing trust [8] . The infrastructure models [9] [10] are based on certificates provided to vehicles. While the self-organizing models [11][12][13] are based on cooperation between vehicles and built on direct, indirect or hybrid trust calculation. For the infrastructure based trust, it could be centralized or distributed trust management. The centralized management presents a single point of failure while the distributed presents challenges due to the lack of infrastructure, openness of wireless links and the highly dynamic network topology [14]. Both models are based on messages correlation or vehicles verification and provide appropriate trust metrics values to vehicles. Based on these trust metric values, nodes can be classified and a secure and reliable communication is established between them in VANET [15].

Similarity mining technique is used for identifying similar messages or similar vehicles [16]-[20]. It is used to recognize the trustworthiness of safety messages. Similarities from different recommenders are used as weights for computing a vehicle's recommendation based reputation.

For the self-organizing (group formation) [21][22], it has the ability to protect privacy, VANET users are anonymous within groups but yet identifiable and accountable to their

group managers. The use of groups simplifies the task of building reputation and calculating trust in the received messages in order to provide better and more confident decisions. Also, it is used for electing the most appropriate group leader by considering the trust value of vehicles.
The proposed solutions designed particularly for VANET partially cover the security requirements [23]. In this paper, we propose a Trust Model based on a secure architecture with cluster formation and GL-based communication. This Trust Model covers major security requirements mentioned in [23]. It is a combination between centralized and distributed cooperation that preserves participants' privacy and maintains low network overhead. It's a real-time processing which provides an inherent secure environment that can mitigate the potential attacks or minimize their duration on VANET [6].

III. PROPOSED TRUST MODEL

We propose a secure and distributed public key infrastructure for VANETs based on a hybrid Trust Model [6]. We adopt a modular architecture defined in [7] and the group formation in [5]. The proposed Trust Model is used to estimate the corresponding trust metric values of participating vehicles. It judges their trustworthiness. Trust metrics value is a combination of direct and indirect calculation, centralized and decentralized authorities and in multi-cases (normal mode or in case of an alert). The node with highest trust metric value is considered the trustiest and will be a potential Group Leader. GLs have crucial roles as they are communicating directly with specific management authorities.
Consider a group of vehicles within a geographical area of 300 meters radius circulating in a cooperative driving as shown in Figure 1.

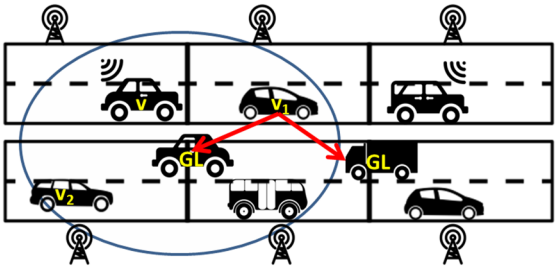

Figure 1.Vehicular groups

Each vehicle v monitors all its 1-hop neighbours. We define:
$T_d v(i)$: "direct trust", judgment of vehicle v on vehicle i.
$T_r v(i)$: "indirect or relative trust", judgment of v on i based on v'neighborhood opinions.
$T_{tot} v(i)$: "total trust" of vehicle i calculated per v (based on direct and indirect trust).
$T_{glob}(i)_0$: initial "global trust" of vehicle i given by RSU for newly cars entering VANET.
$T_{glob}(i)$: "global trust" of vehicle i stored in RSU.

A. Scenario

A new vehicle *i* entering the geographical area will authenticate to an RSU (for mutual authentication). It will get its certificate obtained from the CA (Certificate Authority) and its initial trust $T_{glob}(i)_0$ that will be modified following its behaviour on the road. So it has $P_u i$, $P_r i$, $Cert_i$, $T_{glob}(i)_0$. Where $P_u i$, $P_r i$ are respectively the public and the private keys of the vehicle i, $Cert_i$ is the certificate of vehicle i, $T_{glob}(i)_0$ is the initial "*global trust"* of vehicle i given by the RSU.
The new vehicle *i* will then join an existing group [5]. It will get the public and private keys of this group Pu_{gr}, Pr_{gr}. It will broadcast beacons for its neighbourhood. The vehicles in the neighbourhood of vehicle *i* will add this car to their Neighbourhood table and record its information in their database. Beacon is issued normally every 100ms, a checker every 2x100ms will update the Neighbour table about the vehicle status (alive or not). The Neighbours table form is shown in TABLE I below:

TABLE I.NEIGHBORHOOD TABLE

Neighbour ID	Contact Time	Status
(Non-clear ID, for privacy)	Time for first beaconing message	If still neighbour or not. If not receiving from it since t>2*100ms, remove from this table to history table.

Each vehicle in the group monitors different metrics/parameters. Certain parameters related to the communication, others related to the transmission/reception of a vehicle, some parameters given by the GPS or sensors, others based on variables calculation. Such metrics can be categorized into: critical, intermediate and optional. Based on these parameters, the calculation of the trust metric of each vehicle is done. This trust metric has a TTL (Time-To-Live) because it is an important indicator in a rapidly changing topology (VANET). It adapts the real-time connection status.

B. Direct Trust Computation:

The direct trust of each vehicle will be calculated by other vehicles in two cases:

i. *Normal case*: beacons are broadcasted between vehicles each 100 ms; those vehicles are directly connected within one hop.
ii. *Event Case*: an event happens (emergency or warning message broadcasts).

In this paper, we focus on Normal case and we present the calculation of the trust metric.

I. *Normal case*

The beacon is composed from: V_{ID}, current position, velocity, status. Where V_{ID} stands for vehicular identity, current position stands for its geographical position, velocity its vehicle driving velocity and status. $T_d(i)$ the direct judgment on vehicle i done by another vehicle will be calculated based on the following equation:

$$\mathbf{T_d(i)} = \left[\prod_{j=1}^{k} \propto_j \boldsymbol{m_j}\right]^{1/k} \quad (1)$$

Where α_j is a weight factor and m_j is the trust metric reflecting one of the k parameters including:

- *Active frequency:* compute the number of received messages from a vehicle every 100ms

- *Velocity* of a vehicle broadcasted in the beacon.
- *Transmission Power* (TP): the greatest TP is, the closest is the vehicle.
- Number of *confident neighbours* N_v.
- *Internode distance* d_i: the distance between the monitored vehicle (i) and the monitoring (v). This distance has a threshold d_{norm} (normal distance expected between two consecutive vehicles). If the internode distance calculated << d_{norm}, vehicle i probably is a malicious one that wants to cause an accident. Otherwise, if the internode distance >> d_{norm}, i tries to slow the traffic to produce congestion.
- *Traffic rules obey*: is a metric calculated for every vehicle at each stop light and got from radar. Those includes:
  - s_i: bypassing speed indicator. How often the vehicle exceeded the speed limit.
  - l_i: changing lane indicator.

Within the proposed Trust Model, the beacon is updated to include the direct trust. Each vehicle broadcasts beacons containing a list of calculated direct trust of all neighbours. Receiving vehicles will register and use these direct trusts later in their indirect trust calculations.

C. Indirect Trust Computation:

The indirect trust is based on the others opinions (the neighborhoods of v). Thus $T_r(i)$ is an average value calculated based on all direct trusts of vehicle i received by v's neighborhood. Within each vehicle v, the indirect trust of a neighbouring vehicle i, is calculated as follow:

$$\mathbf{T_r(i)} = \frac{1}{N}\sum_{j=1}^{N} T_d^j(i) \quad \textbf{(2)}$$

Where j: vehicles neighbours to vehicle v.
N: set of beacons that contain the direct trust of (i), $T_d(i)$.
$T_d^j(i)$: direct trusts of (i) calculated by vehicles j, will intervene in the calculation of indirect trust of vehicle (v) over vehicle (i).

D. Total Trust Computation:

The total trust combines the direct and indirect trust for any vehicle. The total trust is calculated at three levels: vehicle, GL and RSU. The total trust basic usage is to define the trustworthiness of a vehicle differently on each level.

a. *Vehicle Level*: the total trust of i calculated by v is given by the following equation:

$$\mathbf{T_{tot}v(i)} = \boldsymbol{\beta_1} * \boldsymbol{T_d(i)} + (\mathbf{1} - \boldsymbol{\beta_1}) * \boldsymbol{T_r(i)} \quad \textbf{(3)}$$

Where 0.5<ß1<1, because each vehicle trusts more its proper calculation.
Every vehicle v contains a database including the direct, indirect and total trusts for all neighbouring vehicles i as shown in TABLE II. i varies from 1 till n. n represents v neighbours.

TABLE II. TRUST DATABASE OF VEHICLE V

Vehicle	$T_d(i)$	$T_r(i)$	$T_{tot}(i)$
i	Direct trust /v	Indirect trust/v	Total Trust /v

At each iteration, old values within the trust database are updated following the smoothing move procedure in the following equation:

New value= α*new value + (1-α)*old value **(4)**

Where 0.5<α <1.
Every vehicle v sends periodically (each 150ms) its neighbouring vehicles total trust list $T_{tot}v(i)$ to the GL which in turn computes the average total trust of vehicles.

b. *GL Level*: The average total trust for vehicle i calculated by a GL, is computed as follow:

$$\mathbf{T_{totm}(i)} = \frac{\sum_{j=1}^{n} T_{tot}^j(i)}{n} \quad \textbf{(5)}$$

Where i: any vehicle within the GL radio range.
n: number of occurrence of vehicle i total trust within the GL database.
$T_{tot}^j(i)$: is the total trust of vehicle i calculated by vehicle j.
The GL sorts periodically its trust list in descending order thus the trusted vehicle is on top of the list. The GL each time passing by an RSU, overloads intelligently the updated total trust $T_{totm}(i)$ only. These vehicles average total trusts participate in the potential GL election process in coordination with the RSU (infrastructure). Therefore, once the GL decided to leave the group, the first in the list (highest trust) will be a GL potential candidate.

c. *RSU Level:* For the i total trust computation, $T_{glob}(i)$, two cases occur:

- Vehicle i belonging to *one group*: $T_{glob}(i) = T_{totm}(i)$ calculated by one GL.
- Vehicle i belonging to *several groups*: RSU calculates the geometric mean of the $T_{totm}(i)$ received for this vehicle i as in "(6)," (e.g. if i belongs to two groups then its $T_{totm}(i)$ will be calculated by two GLs).

$$\mathbf{T_{glob}(i)} = \left[\prod_{k=1}^{N} T_{Totm}(i)\right]^{1/N} \quad \textbf{(6)}$$

N: number of groups to which vehicle i belongs.

RSU (infrastructure) as big data-center will merge and update these trust metrics using the smoothing move procedure mentioned in "(4)," above and result a global trust metric for each node. This global trust metric is used for node trustworthiness evaluation.

IV. EFFICENY OF THE PROPOSED TRUST MODEL

The proposed Trust Model presents many assets listed below:

- The model is a combination between centralized and decentralized network and communication. The centralization resides in the RSU and the security infrastructure while for the decentralization it's based on vehicles and GLs cooperation. This strengthens the solution because it eliminates the drawbacks of the centralized models mainly the delay. The group formation is one of the basic solution for these drawbacks; it is adopted in this model [5][6] and lessens the delays due to the periodical contact between vehicles and infrastructure which cause an exhaustion of infrastructure resources.

- The security requirements are guaranteed by using: the certificates, asymmetric keys (P_ui, P_ri) for authentication, group keys (Pu_{gr}, Pr_{gr}) for anonymous signature (on behalf of the group), while privacy is preserved by using anonymous keys changing frequently offline[5][7].
- Trustworthiness of participating nodes in VANET is evaluated.
- Security attacks are mitigated [6].
- Stability and reasonable convergence of the system is available for GL election.

V. SIMULATION RESULTS

For the simulation, we used GrooveNet v2.0.1 [24], an open source hybrid simulator which integrates mobility and network simulator. It simulates communication among vehicles and has the capability to load a real street map form Tiger / Line database. Multiple broadcast messages are supported to mention the vehicle position for neighbors, vehicle emergency and warning messages. To simulate our proposed Trust Model, we added specific procedures to calculate the trust metric of vehicles. Each simulation was run for 15 minutes in sparse, medium and dense mode respectively with 20, 50 and 100 circulating vehicles. As mentioned in subsection III-B, we consider Normal case.
Initially, the vehicles are randomly positioned within a 0.2-0.5 km² area around the 333 7th Ave, New York, location. Interacting vehicles are allowed to move using the Car Following Model (following their GL) within a maximum distance of 1 km and to return to initial position using the Sight Seeing Trip Model. The transmission range of vehicle radio is 200 m. Vehicles are considered with initial global trust $T_{glob}(i)_0$ = 0.1. Group Leader is moving based on a Uniform Speed Model varying ± 25% of the speed limit of the mentioned street. During this simulation, the parameters ß1and α1 for "(3)," and "(4)," are taken ß1=α1=0.7. Also, without loss of generality, for "(1)", we consider one of the k parameters, which is the velocity of the vehicle.

In our simulation, we consider several scenarios to show the efficiency of the proposed Trust Model:

a. *Variation of Total Trust of vehicles:* in Figure 2, we show the Total Trust Ttot(i) variation of five vehicles spread over the y-axis within a period of 15minutes relatively spread on the x-axis. Vehicle total trust varies based on the vehicle behavior within VANET. It starts with 0.1 and can reach 0.9 for the most trusted vehicles. At time 0, all vehicles (v5, 7, 31 and 33) started with $T_{tot}(i)_0$ their initial value 0.1, then the proposed model based on the cooperation between vehicles calculates the updated trust metric for these five vehicles based on their behavior. We can notice for example, v7 after 4.5 minutes; its total trust increased to 0.83 and remains unchanged due to its good behavior until the end of the simulation. While for v5, its total trust increases after 1.5minutes to 0.7 for a duration of 10.5minutes then to increase to 0.76 then decrease to 0.5 at the end of the simulation. All these values reflect the real vehicles behavior. This is a snapshot taken from our multi-cases simulation in medium mode.

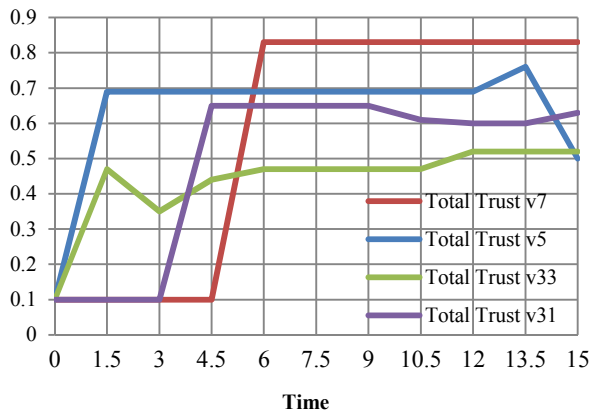

Figure 2. Variation of Ttot(i) for 5 sample vehicles - medium mode

b. *Model-Group Formation:* in Figure 3, we show that the Trust Model security architecture (GL formation) overcomes the PKI infrastructure in the network overhead. We took an example of safety message dissemination, at different snapshots within 15 minutes duration. We noticed that in our model, the authenticated vehicles within the same group disseminate directly these safety messages without returning to the PKI infrastructure to authenticate their neighbors.

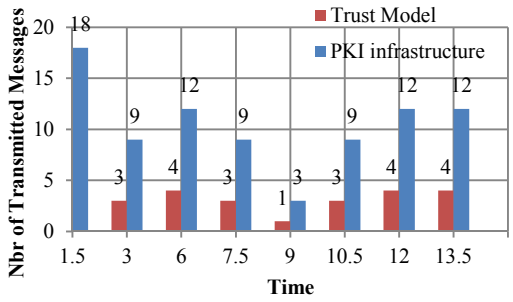

Figure 3.Comparison of transmitted messages/vehicle in PKI vs Trust Model architecture

As example in Figure 3, after 6 minutes from the simulation start, one of the vehicles had 4 neighbors, it notifies them about the accident by sending 4 messages exactly. While in PKI infrastructure, it should authenticate first each neighbor with the RSU then send it the safety message which result 3messages/vehicles in total 12 messages for 4 neighbors.

c. *Model Behavior for GL Election:* within our simulation, we focus on the highest three trust value to elect the candidate GL. Let us take 10 snapshots of the simulation done above, in Figure 4 from minutes 5 till 15. In

snapshot 3, potential GL1 is vehicle 20, the second potential GL2 is vehicle 15 and the third is vehicle 17. At snapshot 4, 5 and 6 the order remains the same which means the same potentials GLs. At snapshot 7, a reordering happens due to behavior changes, but candidate GL1, vehicle 20 remains the pioneer till the end of this simulation. The stability of the system in GL election was clearly revealed within this simulation and other ones. This reflects stability in GL behaviors within VANET.

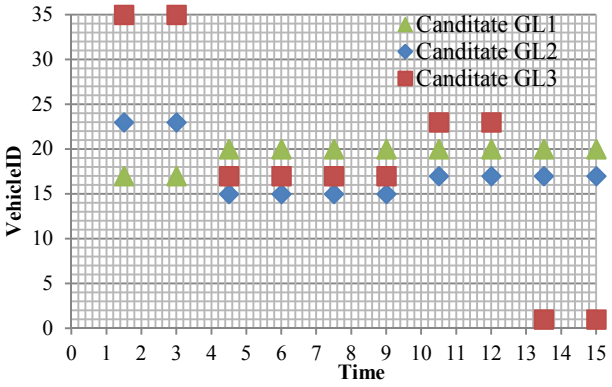

Figure 4.Candidate GLs

VI. CONCLUSION

In this paper, we proposed a Trust Model based on a secure architecture with cluster formation and GL-based communication. Through simulations we showed how this model helps to elect GLs. The trust metric is updated according to the instantaneous behavior of the vehicles.

Future work will evaluate the proposed model by investigating issues like specific frequent attacks (Sybil, Blackhole), multi-groups interaction and the case of an event.

REFERENCES

[1] H. Hasrouny, A.E. Samhat, C. Bassil and A. Laouiti, "VANET Security Challenges and Solutions: A Survey", published in Vehicular Communications journal, Elsevier, Vol.7, pp. 7-20, January 2017.

[2] ETSI TS 102 940 V1.1.1- ITS - Communications security architecture and security management.

[3] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments: IEEE Std 1609.2™-2012

[4] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin and T. Weil, "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions", published in Communications Surveys & Tutorials, IEEE (Volume:13 , Issue: 4), pp. 584-616, July 2011.

[5] H. Hasrouny, C. Bassil, A.E. Samhat and A. Laouiti, "Group-based authentication in V2V communications", in Proc. of IEEE Fifth International Conference on DICTAP, pp. 173-177, 2015.

[6] H. Hasrouny, C. Bassil, A.E. Samhat and A. Laouiti, "Security Risk Analysis of a Trust model for Secure Group Leader-based communication in VANET", in Ad-hoc Networks for Smart Cities Book, IWVSC Malaysia, Springer, Ch.6, pp. 71-83, 2016.

[7] W. Whyte, A. Weimerskirch, V. Kumar and T. Hehn, "A Security Credential Management System for V2V Communications", IEEE Vehicular Networking Conference, pp. 1-8, 2013.

[8] N. Patel and R. Jhaveri, "Trust based approaches for secure routing in VANET: A Survey", Procedia Computer Science, vol. 45, pp. 592–601, Elsevier, 2015.

[9] F. Gómez Mármol and G. Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks", Journal of Network and Computer Applications, vol. 35, no. 3, pp. 934–941, 2012.

[10] A. Zhou, J. Li, Q. Sun, C. Fan, T. Lei and F. Yang., "A security authentication method based on trust evaluation in VANETs", EURASIP Journal onWireless Communications and Networking, Springer, 2015. Available online at: http://link.springer.com/article/10.1186/s13638-015-0257-x.

[11] Z. Liu, J. Ma, Z. Jiang, H. Zhu and Y. Miao, "LSOT: A Lightweight Self-Organized Trust Model in VANETs", Mobile Information Systems journal, 2016. Available online at: https://www.hindawi.com/journals/misy/2016/7628231/

[12] B. K. Chaurasia and Sh. Verma, "Trust Based Group Formation in VANET", MTTER Volume 2, Issue 2, pp. 121-125, April 2013.

[13] A. Tajeddine, A. Kayssi and A. Chehab, "A Privacy-Preserving Trust Model for VANETs", 10th IEEE International Conference on Computer and Information Technology (CIT), pp. 832-837, 2010.

[14] Kavitha . M , Sh. S.Tangade and S. S. Manvi, "Distributed Trust & Time Management Strategy in VANETs", Published in IEEE International Conference on Computing Communication and Networking Technologies (ICCCNT), India, pp. 1-6, 2013.

[15] T. Gazdar, A. Benslimane, A. Rachedi and A Belghith, "A trust-based architecture for managing certificates in vehicular adhoc networks", Published in IEEE International Conference on (ICCIT), pp. 180-185, June 2012.

[16] N. Yang, "A similarity based trust and reputation management framework for VANET", International Journal of Future Generation Communication and Networking Vol. 6, No. 2, pp. 25-34, April, 2013.

[17] A. Rehman, A. Ali, R. Amin and A. Shah, "VANET Thread Based Message Trust Model", Published in IEEE Eight International Conference on Digital Information Management (ICDIM), pp. 55-57, 2013.

[18] H. Xu, L. Hua, Y. Ning and X. Xue, "Detecting the Incorrect Safety Message in VANETS", Research Journal of Applied Sciences, Engineering and Technology 5(17): 4406-4410, 2013.

[19] R. R. Sahoo, R. Panda, D. K. Beherab and M. K. Naskarcm, "A TRUST BASED CLUSTERING WITH ANT COLONY ROUTING IN VANET", Third International Conference on Computing Communication & Networking Technologies (ICCCNT), pp. 1-8, 2012.

[20] A. Ltifi, A. Zouinkhi and M. S. Bouhlel, "Trust-based Scheme for Alert Spreading in VANET" ,The International Conference on Advanced Wireless Information, and Communication Technologies (AWICT), Vol. 73, pp. 282-289, 2015.

[21] Q. Ding, M. Jiang, X.. Li and X. Zhou, "Reputation-based Trust Model in Vehicular Ad Hoc Networks", Published in IEEE International Conference on Wireless Communications and Signal Processing (WCSP), pp. 1-6, 2010.

[22] X. Li, J. Liu, X. Li, and W. Sun, "RGTE: a reputation-based global trust establishment in VANETs," in Proceedings of the 5th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS '13), pp. 210-214, China, 2013.

[23] Q. Alriyami, A. Adnane and A. K. Smith, "Evaluation Criterias for Trust Management in Vehicular Ad-hoc Networks (VANET)", International Conference on Connected Vehicles and Expo (ICCVE), pp. 118-123, 2014.

[24] GroovNet v2.0.1, Vehicle Network Simulator, Second International Workshop on Vehicle-to-Vehicle Communications (V2VCOM), San Jose, USA. July 2006, https://github.com /mlab/GrooveNet .

