2013 International Conference on Communication Systems and Network Technologies

Trust Computation in VANETs

Brijesh Kumar Chaurasia
ITM University,
Gwalior (M.P.), India
bkchaurasia.itm@gmail.com

Shekhar Verma
IIIT Allahabad,
Allahabad (U.P.), India
sverma@iiita.ac.in

Geetam S Tomar
Machine Intelligence Research Labs
New Jiwaji Nagar, Gwalior, India
gstomar@ieee.org

Abstract—**In this work, we study the application of Perron–Frobenius theorem for computing trust in the VANET environment. Safety critical and safety related messages in a VANET can lead to major changes in the behavior of vehicles moving on the road which can prevent unpleasant traffic situations. False messages can result in serious conditions like collisions. Trust management in VANETs is necessary to deter broadcast of selfish or malicious messages and also enable other vehicles to filter out such messages. A decentralized dynamic trust management system must be scalable with an ability to cope with sparsity of direct interactions. In this work, it is shown that messaging behavior of vehicles can be modeled as a primitive graph. This allows the application of Perron–Frobenius theorem. It is found that the eigenvalues of the matrix corresponding to the interaction graph can be used to compute trust values in the VANET setting.**

Keywords- Trust management; VANET; ranking;

I. INTRODUCTION

Vehicular ad hoc network (VANET) is a network of vehicles [1] in which vehicles moving on the road broadcast messages to provide the safety and comfort to the users. VANET is highly disconnected, high mobility network in which nodes have ample computational energy and storage capacity. The network is characterized by continual change in the neighborhood around a vehicle, V2V messages and limited infrastructure support [2]. Since the vehicles exchange critical information, a malicious vehicle may inject false messages with different identities. This may trap a vehicle into taking wrong decision with dire consequences. Security becomes a prime concern in VANETs and necessitates authentication of entities and the messages. The vast distributed nature of the network coupled with the ephemeral neighborhood makes it difficult to discover or penalize a misbehaving vehicle. This may tempt even an honest vehicle to inject false information into the network or forwarding messages to gain temporary traffic comfort. This limits the use of cryptographic measures for verifying the veracity of a message in the VANET scenario. This necessitates trusting the vehicle transmitting the message and on the message itself for believing on a message before taking action. The question is how to trust a message sent by another vehicle. Trust establishment between vehicles is, therefore, a major challenge to be solved to ensure the trustability of messages [3]. This problem is aggravated in the vast expanse of the vehicular ad hoc network in which a vehicle may need to act on the message of a vehicle which it has never interacted with before.

Trust is a subjective one way binary relation between the trustor and trustee in which the trustor attaches a value to the trustee [4]. The value can range from -1 to 1 (zero indicates no trust) representing distrust to trust. The trust is bound to the expected behavior of the trustee to a specific objective. For different objectives, the trust value may be different for the same trustee. The perception of the trustor embodied in the trust value is a function of evaluation criteria and local state of a trustor. The local state of an entity is unique to the trustor and independent of other entities in the system. Information received from other entities can affect the local state of an entity [5]. A trust chain can be formed if the trust can be transferred along the chain [6]. Trust transfer is possible only from t_1 to t_2 only if t_2 trusts t_1 and the predicates used by t_1 to trust an entity e is known to t_2. To make trust transferable, t_1 must know t_2's trust attitude and trust policy. The t_1 must be ready to believe t_2 and accept its recommendations. Belief on t_2 depends on its credentials and reputation. A credential is an assertion on the trustee's attributes which may be based on cryptographic material. Reputation is the aggregation of trust opinions of a vehicle from the VANET community [7]. Both trust and distrust are therefore transferable.

In a VANET, certificate issued by a centralized trusted authority can be used to verify the authenticity of a vehicle [8]. However, selfish action by authenticated vehicles is a distinct possibility in a VANET. Thus, a certificate must be time limited but this cannot solve the problem completely. Limited access to infrastructure and associated time delays requires dependence of vehicles moving on the road for trust establishment. Dynamic group formation with trusted vehicles on the road can be used for as one of methods for trust generation of vehicles [9]. But, the trust generation for becoming a part of a group is itself time consuming. Other methods like experience based, role based trust establishment and situation aware trust establishment have been proposed in literature that subsume different types of information for generating trust value for a vehicle. Most of the methods are based on reputation based techniques [10]. In the present study, a method that uses direct interactions, recommendations of other vehicles and messages is proposed. The method is based on Perron-Frobenius (PF)

978-0-7695-4958-3/13 $26.00 © 2013 IEEE
DOI 10.1109/CSNT.2013.103

[11] theorem has been used for generating trust values. The rest of the paper is organized as follows. Section II contains the problem definition followed by the proposed methodology in section III. Section IV concludes the paper.

II. Problem Definition

The trust establishment process in a VANET must take into consideration the direct messages, forwarded messages from vehicles, its own observation of the environment, aggregated recommendations of other vehicles about a vehicle and messages and the nature of messages. All these must be used in the trust establishment of a vehicle and the associated messages before acting on the message sent by it. This requires a method that can not only take all the parameters into consideration but is also able to generate trust values in the absence of a majority of the parameters especially lack of direct trust.

III. Proposed Method

In a VANET, a trustor observes its immediate environment, receives messages from vehicles that have also observed the same events, receives messages from nodes that have forwarded these messages, rates the trustees, and makes recommendations about the trustees to other vehicles. When a vehicle is required to make a decision, it checks its direct trust values and uses recommendations given by trustworthy vehicles to decide whether it will undertake a given action. This decision is also subject to the evaluation of the data before final action is taken. The evaluation of data is important as veracity of messages in VANET is context dependent. Message veracity is subjective and spatio-temporal notion. A message may be true for one vehicle and not for others depending on the message delay. The situations on the road vary with time. For example, a traffic perturbation may occur and vehicles observing this condition broadcast messages reporting the event. The perturbation may be over before a vehicle which has received the messages reaches the condition site. The spatio-temporal context requires vehicles to associate and compute the uncertainty in the veracity of messages. This locality of the context entails that trust evaluation process to emphasize on recent information. Moreover, in a VANET, there are different kinds of messages ranging from benign to safety critical messages. The relative importance of messages must also be considered in trust evaluation. The trust value attached to a trustee by a trustor is a function of trustor's own opinion of the trustee, opinions of trustor's neighbors, the trustworthiness of neighbors and trust associated with the messages.

A. Trust Computation

The trust computation method is based on Perron–Frobenius theorem [11] in the VANET environment based on types of messages, direct interaction with vehicles, aggregated recommendation from other vehicles and content of the messages are used.

Table 1. Trust value description of messages

S. No.	Message Category	Example	Trust Value Message Strengths
i	Safety Critical messages	Crash-Pending Notification, Hard-Brake (Collision Warning, EEBL, LANE changing , Anti -Lock, etc.) and Control Loss	5
ii	Safety Related messages	Emergency Vehicle Approaching, Probable-situation (e.g., Rapidly deteriorating dangerous conditions), SPAT (Signal Phase and Timing)	4
iii	Non-Safety application	Electronic Toll Tax Collection	3
iv	Non-Safety messages	Location based services : Car parking information, Off-Board Navigation Reroute Instructions, Location finding	2
v	Non-Safety messages	Infotainment services : Digital Map Download, songs and games downloading services	1
vi	Beacons	Locations related information etc.	1/2

Perron Frobenius Theorem: Let A be a non-negative irreducible matrix with spectral radius $\rho(A)$. Then, the following properties are satisfied :

(i) $\rho(A)(> 0)$ is an eigenvalue of $\rho(A)$ with multiplicity one,

(ii) The left and right eigenvectors associated to $\rho(A)$ are (strictly) and for any other eigenvalue λ of A, $|\lambda| \leq \rho(A)$

If the value of trust ranges from 0 to 1, then the trust relation between vehicles will form a non-negative irreducible matrix will vehicles as vertices and edges between two nodes will exist if there is direct interaction. The edge weights will be decided on the message strength and number of messages transferred between nodes. Message strength depends upon message type as given in Table 1. In the proposed direct ranking trust computation method, each participant vehicle can compute trust value based on the message transfers with other vehicles. The computed trust value depends on the veracity of messages as verified by the vehicle using its own observations of the environment, strength of messages and reputation given by other vehicles. Thus, in the proposed scheme, trust computation can be divided into three categories. Direct trust computation, indirect trust computation and reputation based trust computation technique.

Direct computation using Perron–Frobenius theorem [11] for computing trust in the VANET environment is based on message strength is propose. In the proposed direct ranking trust computation method, each participant vehicle can compute trust value based on the messages received from other vehicles. The computed trust value depends on both the outcome of the message veracity and strength of messages. If we suppose there exists a vector of ranking value r, with positive message strength r_j indicating the strength of the j^{th} participant vehicle's transmitted message, then we define a trust computation for i^{th} participant vehicle as

$$s_i = \frac{1}{n_i}\sum_{j=1}^{N} a_{ij}\, r_j$$

Where a_{ij} is some nonnegative number depending on the outcome of the message transaction between participant vehicle i and the participant vehicle j, N is the total number of vehicles participated in transactions among themselves, and n_i is the number of the message communicated by participant vehicles i. If message is communicated just after authenticated by any mechanism in VANET, the value of n_i should be more, after that it should be decreased after a period of time. For example, for one transaction we could pick a_{ij} to be 1 if message is correct, zero if message information is incorrect and ½ if message is beacon (gives only location information). For a vehicle, we can pick a_{ij} to be 5 if message is safety critical, 1 if message is non-safety. If message gives right information then value will be positive and if message is false, then the value will be zero.

Another method is to distribute the one value per transaction between vehicles in a continuous, rather than discrete way. One way to assign a value to a_{ij} is to distribute the point on the basis of the message strength. If vehicle i receives S_{ij} points (weighted sum of correct messages) and S_{ji} points (weighted sum of incorrect messages, (weights being different for correct and incorrect message of same priority)) during a communication session. Then,

$$a_{ij} = h\left(\frac{S_{ij}+1}{S_{ij}+S_{ji}+2}\right),$$

For example, vehicle i communicates with the vehicle j. There are two cases arise. First, if vehicle receive same message from other vehicles with reputation of j^{th} vehicle and secondly, if vehicle receives different messages from same j^{th} vehicle. Trust computation are as follows:

Case 1: j^{th} vehicle sent safety critical message having strength 5. So, a_{ij} is 0.875.

Vehicle i receives the message from other vehicle and receives j^{th} reputation is 2, 3 and 5. Then the rank of vehicle j by vehicle i is:

$$r_i = \frac{1}{n_i}\sum_{j=1}^{N} f(a_{ij}\, r_j)$$

Where a_{ij} is some nonnegative number depending on the outcome of the message transaction(s) between participant vehicle i and the participant vehicle j, N is the total number of vehicles participated in transactions among themselves, and n_i is the number of the message communicated by participant vehicles i. And f is some continuous monotone increasing function with $f(0) = 0$, and $f(\infty) = 1$.

$$r_1 = 0.875 \times 2 = 1.75$$
$$r_2 = 0.875 \times 3 = 2.625$$
$$r_3 = 0.875 \times 5 = 4.375$$

So, the actual rank of the j^{th} vehicle is:

$$r_i = \frac{1}{3}(8.75) = 2.9166$$

The proposed rank is based on the strength of the messages the communication among the vehicles.

Similarly, if vehicle vehicle i communicates with the vehicle j and j^{th} vehicle sent beacon message having strength 1/2. So, a_{ij} is 0.60. Vehicle i receives the message from other vehicle and receives j^{th} reputation is 2, 1, 2 and 4. Then the rank of vehicle j by vehicle i is:

$$r_1 = 0.60 \times 2 = 1.20$$
$$r_2 = 0.60 \times 1 = 0.60$$
$$r_3 = 0.60 \times 2 = 1.20$$
$$r_4 = 0.60 \times 4 = 2.40$$

So, the actual rank of the j^{th} vehicle is:

$$r_i = \frac{1}{4}(5.40) = 1.35$$

Case 2: j^{th} vehicle sent safety critical message, non safety message and beacons having strength 5, 3 and ½ respectively. So, a_{ij} is 0.875, 0.667 and 0.60.

Vehicle i receives the messages from same vehicle and receives j^{th} reputation is 2. Then the rank of vehicle j by vehicle i is:

$$r_i = \frac{1}{n_i}\sum_{j=1}^{N} f(a_{ij}\, r_j)$$

$$r_1 = 0.875 \times 2 = 1.75$$
$$r_2 = 0.667 \times 2 = 1.33$$
$$r_3 = 0.600 \times 2 = 1.20$$

So, the actual rank of the j^{th} vehicle is:

$$r_i = \frac{1}{3}(4.28) = 1.426$$

From the above illustration, it can be observed that the Perron Frobenius Theorem can be used to associate trust values with vehicles. The mechanism is able to consider different types of information for computation of the trust values.

IV. Conclusion

VANET becomes useless if a vehicle cannot accept the veracity of message and act on a message broadcast in the network. The acceptance of VANET is, therefore, relies on the implementation of a successful trust evaluation system. The sparsity on direct interactions, availability of forwarded messages, reliance on an ever-changing neighborhood, event specific, location and time sensitive message data necessitated a trust evaluation technique that could work with the available data. The proposed PF theorem based method is able to work with full or partial data to generate trust values. In future work, we aim to perform experiments to evaluate its performance in real world scenarios.

References

[1] S. Yousefi, M. Mousavi and M. Fathy, "Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives", In proceedings of the 6th International Conference on ITS Telecommunications (ITST2006), pp. 761 - 766, 2006.

[2] W. Xiang, Y. Huang and S. Majhi, "The Design of a Wireless Access for Vehicular Environment (WAVE) Prototype for Intelligent Transportation System (ITS) and Vehicular Infrastructure Integration (VII)", Vehicular Technology Conference, VTC 2008-Fall. IEEE 68th, pp. 1-2, Sep 2008.

[3] J. Breuer, A. Held, T. Leinmller and L. Delgrossi, "Trust Issues for Vehicular Ad Hoc Networks", In 67th IEEE vehicular technology conference (VTC2008-Spring), pp.2800-2804, 2008.

[4] Yu Yanli, Li Keqiu, Zhou Wanlei and Li Ping, "Trust Mechanisms in Wireless Senor Networks: Attack Analysis and Countermeasures", In Journal of Network and Computer Applications, pp. 1-14, 2011.

[5] S. Eichler, "A Security Architecture Concept for Vehicular Network Nodes", In 6th International Conference on Information, Communications & Signal Processing, pp.1-5, 2007.

[6] M. El Zarki, S. Mehrotra, G Tsudik and N. Venkatasubramanian, "Security Issues in a Future Vehicular Network", In European Wireless, pp. 270–274, 2002.

[7] M. Gerlach, "Trust for vehicular applications," In Proc. 8th Int. Symp. Auton. Decentralized Syst., pp. 295–304, 2007.

[8] Umar Farooq Minhas, Jie Zhang, Thomas Tran, and Robin 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.

[9] B. K. Chaurasia and Shekhar Verma, "Trust Based Group Formation in VANET," In Modern Traffic and Transportation Engineering Research, 2013. (Accepted)

[10] A. Jøsang and R. Ismail, "The beta Reputation System," In Proc. 15th Bled Electron. Commerce Conf., pp. 324–337, 2002.

[11] J. P. Keener, "The Perron-Frobenius Theorem and Ranking of Football Teams," SIAM Review, Vol. 35, No. 1, pp. 80-93, 1993.