Journal of Electronics and Information Science(2017) 2: 107-111
Clausius Scientific Press, Canada

Trust Models in VANETs

Gu Xiang

School of Computer Science and Technology, Nantong University, Nantong 226019, China
gu.x@ntu.edu.cn

Keywords: VANET, Trust Model, Entity-Oriented Models, Data-Oriented Models

Abstract: The paper introduces trust models in VANETs. A vehicle is able to identify facticity of messages that are received by using a trust model. Models are generally divided into three categories, which are entity-oriented models, data-oriented models and combined models. This paper discusses some typical models in different categories and gives short comments on them. Kinds of advantages and weaknesses of models that are pointed out in the paper have some reference value for the future designing.

1. Introduction

The concept of "Trust" is originated from sociology filed. One person can infer the next behavior of another person based on his previous behaviors. In another word, a person may continue behaving well or bad just as he always does in next time. The concept is also introduced into other fields such as electronic commerce, online shopping and so on. Now many efforts have been done to apply concept "trust" into VANETs (Vehicular Ad Hoc Networks) by many researchers. By using trust models, a vehicle can judge the trustiness of messages which it receives from other vehicles in VANETs. It can also detect those dishonest or malicious vehicles and get rid of them. That means it can refuse to communicate with those identified vehicles and ignore mendacious data from them. Furthermore, trust models are useful in incenting honest vehicle to take part in communicating among a VANET and discouraging vehicles' self-interested behaviors.

2. Using Trust in VANETs

There are two important characters of concept "Trust" which must be considered seriously while designing a trust model. The first one is partially transitive. For example, node A trusts B and B trusts C, while we cannot infer that node A can also trusts C completely. This is the knowledge base of trust recommendation. B can recommend his knowledge about C to A, and A will take B's recommendation into account while computing the trust value of C. The second one is that the trust is content relevant, which means A cannot trust B will win in a swimming game although B is very famous for his long-distance running ability. This is why a trust model always identifies trust as behavior trust and recommendation trust.

Some other issues should also be considered while designing a trust model in VANETs. Firstly, Events on road themselves are dynamic. Secondly, the topology of a VANET is dynamic. And lastly, the scale of a VANET may change greatly. All of those factors will affect the validity and accuracy of a trust model.

There are two typical frameworks of trust models in VANETs. One is centralized and another is decentralized. In a centralized framework, there is a manage center to take charge in calculating all vehicles' trust values just as Fig. 1 shows. While in a decentralized framework, as Fig. 2 shows, a vehicle has to observe other vehicles' behaviors and calculates their trust values by itself.

A well designed trust model should be able to help to resist typical attacks in a VANET such as Sybil attack, on-off attack, Bad-mouth attack, newcomer attack, collusion attack and so on. A trust value can be expressed as a real number among (0, 1) or an integer number among [0, 50] or just a discrete value such as (not trust, little trust, trust, very trust). Different models adopt different expression according to their calculating algorithms.

Many trust models in VANETs have been proposed. Those models can be categorized into three kinds. The first one is entity-oriented models, the second one is data-oriented models, and the third one is combined trust models.

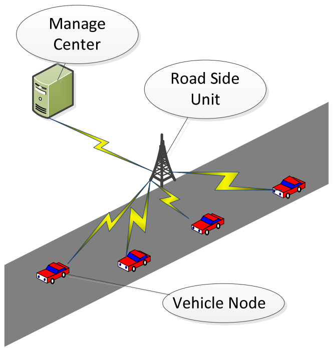


Fig.1 Centralized Framework

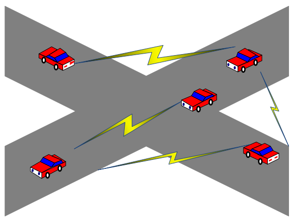


Fig.2 Decentralized Framework

- Many trust models in VANETs have been proposed. Those models can be categorized into three kinds. The first one is entity-oriented models, the second one is data-oriented models, and the third one is combined trust models.

3. Entity-oriented Trust Models

A message can be trust if it is emitted by a trusted vehicle. That is the general feature of entity-oriented trust models. Some of those models are based on vehicles' role; others are based on experiences / observations, just as Fig.3 shows.

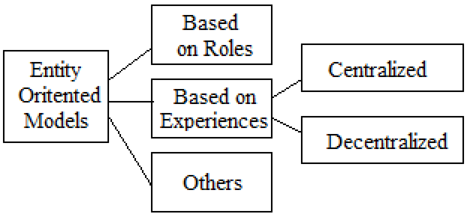
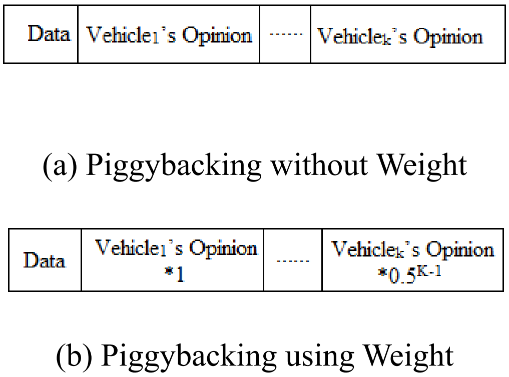


Fig.3 Entity Oriented Trust Models



Data	Vehicle$_1$'s Opinion	......	Vehicle$_k$'s Opinion

(a) Piggybacking without Weight

Data	Vehicle$_1$'s Opinion $*1$	......	Vehicle$_k$'s Opinion $*0.5^{K-1}$

(b) Piggybacking using Weight

Fig.4 Piggybacking Message

Vehicles' roles can be categorized as authoritative vehicles, official vehicles and ordinary cars [1]. Authoritative vehicles mainly refer to police cars who undertake the responsibility for the traffic. Other information publishers such as bulletin boards which are controlled and managed by traffic governments can also be looked as authoritative ones. Those nodes are awarded the highest trust rank. All information from those nodes will be accepted absolutely. Trustiness of official vehicles is lower than authoritative ones. Messages from those vehicles will be adopted in most occasions. Ordinary cars have the lowest trust values. Those cars are owned and driven by general public and they are in great numbers. Messages generated by them must be carefully identified before they are accepted. As the number of authoritative vehicles and official vehicles is much less than ordinary cars, a lot of vehicles named anchor nodes are pre-authenticated and they can be trustful.

Centralized experience-based trust models usually include three parts, RMC (Reputation Management Center), RSU (Road Side Units) and vehicle nodes. The architecture is shown in Fig.1. RMC is responsible for computing trust values of all vehicles in a VANET. Each vehicle on road will monitor its neighbors' behaviors and reports its observations to the RMC. The RMC update vehicles' trust values periodically according to reports it received. If a vehicle marked as Alice wants to publish a message, it should append its trust value, which is gotten from the RMC and encrypted by the RMC's private key, to that message [2]. As the trust value is encrypted, Alice has no ability to modify the value. When another vehicle, for example named as Bob, received the message, it can parse Alice's trust value by using the public key of the RMC and then it can decide whether trust or distrust the message according to Alice's trust value.

But there is an attack risk which is known as bad-mouth in such models. The RMC can adopt statistic methods to resist such an attack. For example, the RMC can look a recommendation about a vehicle as a random variable. According to central limit theory; those recommendations should obey standard normal distribution [3]. Then those recommendations which are too far away from the center will be looked as malicious ones and then be ignored.

β-distributed model is a kind of typical model of decentralized experience-based models [4]. Suppose vehicle i is a neighbor of vehicle j, and i observes j's behaviors for a certain time. Then i can get its direct trust value Ti,j about j, just as formula (1) shows.

$$R_{i,j} = \frac{\alpha}{\alpha + \beta + 1} \qquad (1)$$

In the above formula, α represents the number of j's good behaviors which are observed by i, and β represents the number of bad behaviors.

All j's neighbors will exchange their direct trust values about j among them, these values are known as indirect trust values. The trust value of j is the synthesis of direct and those indirect values. If there is an ephemeral lost between i and j, a fade factor will be applied to formula (1) while i is calculating its direct trust value about j.

Another concept which is often used in distributed models is similarity. Characters of vehicle is marked as an n-dimensions vector (Speed, Direction, Position,……) [5]. Similarity between two vehicles is based on Euclidean distance, which can be calculated according to formula (2).

$$w = \frac{1}{(\sum_{i=1}^{n}(X_i - Y_i)^2 / n)} \qquad (2)$$

After using the similarity, indirect trust values can be synthesized as formula (3). Suppose vehicle i is calculating the trust values of vehicle j, and i receives recommendation about j form its neighbor k. The similarity between i and k is $w_{i,k}$, i's trust value about k is $R_{i,k}$ and k's recommendation about j is Rk,j. Then i can get its indirect trust value $C_{i,j}$ about j.

$$C_{i,j} = \frac{\sum_{k=1,\ldots,n,\, k\neq i}(w_{i,k} \times R_{i,k} \times R_{k,j})}{\sum_{k=1,\ldots,n,\, k\neq i}(w_{i,k} \times R_{i,k})} \qquad (3)$$

From the direct trust value and indirect trust value, i can get its trust value about j according to formula (4).

$$T_{i,j} = \beta R_{i,j} + (1 - \beta)C_{i,j} \qquad (4)$$

4. Data-oriented Trust Models

Different from entity-oriented models, whether the messages will be accepted by a receiver is depended on the message itself instead of the message sender.

Piggybacking method is a typical data-oriented model [6]. A message which announces a certain event happened is published by a vehicle in a VANET. The messages will be received by many vehicles and then most receivers will forward it according a certain rule. Each forwarder appends its own opinion to the message; this opinion is formed on the basis of its own observation and previous opinions which are attached by previous forwarders, just as Fig.4 shows. One shortcoming of this method is that those early opinions have more influence because those opinions will be repeatedly cited by latter forwarders. One effective improvement of this method is that different vehicles' opinions have different weight. A vehicle's position is closer to the event; the weight is larger.

Another typical method is voting. Each vehicle that drives through the event place will send out a message to announce whether the event is happened or not. Behind vehicles will receive a lot of such reports from different vehicles who have already passed the place. Then they can make a decision whether it should accept the event. Strategies of decision making include fresh message priority that means new messages have larger weight, majority wins that means most vehicles' opinion will be adopt, majority of freshest X that means not only the number of vehicles who say 'yes' but also the freshness of opinions will be taken into account.

Bayesian inference method is also a method which is studied by many researchers [7]. Suppose e is a set of reports a vehicle received. It is expressed as e={e1,e2,e3,……,ek}. And report e1 can be expressed as $\mathrm{e}_1 = \{\mathrm{e}_1^1, \mathrm{e}_1^2, \dots, \mathrm{e}_1^{\mathrm{i}}, \dots, \mathrm{e}_1^{\mathrm{I}}, \}$, that means e1 announces events a1,a2,…,ai,…al. Assume the prior probability of event ai is P[ai]. After a report set e is received, the posterior probability of event ai can be calculated according to formula (5).

$$P[a_i|e] = \frac{P[a_i]\prod_{k=1}^{K} P[e_k^j|a_i]}{\sum_{h=1}^{I}(P[a_h]\prod_{k=1}^{K} P[e_k^j|a_h])} \text{ ,} where\ P\left[e_k^j\middle|a_i\right] = \begin{cases} P[e_k^j|a_i], & j = i \\ 1 - P[e_k^j|a_i], & j \neq i \end{cases} \qquad (5)$$

5. Comments and Conclusion

Generally speaking, entity-oriented trust models can make a quick decision as they only need to identify who publishes a message. Centralized models usually need a very powerful center to deal with all vehicles' trust values; sometimes it is necessary to adopt a distributed method in the implementation. While decentralized models seldom consider dynamic topology of a VANET. They always assume a vehicle has enough time to observe another vehicle to collect plenty of evidence to calculate a trust value. But in fact, this assumption is almost impossible as a communication link between two vehicles is so easy to lose due to their high speed and near random running direction.

As to data-oriented models, they cannot work as soon as entity-oriented models because they have to collect evidences from others. Furthermore, a vehicle has to identify every message it received separately. This increases the computation burden of vehicles in a VANET. But decentralized data-oriented models are easy to be implemented compared with decentralized entity-oriented models as vehicles not need to keep a stable link with others. A prominent problem in voting methods is that it is very difficult to resist collusion attack. One is hard to identify those false messages which are emitted by a group of malicious vehicles. In Bayesian approach models, all possibilities must form a complete set but few researchers notice that condition and this makes their models unreliable.

Just as we mentioned, some combined trust models have already been proposed. Although these models improve reliabilities; but at the same time they increase the calculation complexity and reduce models' efficiency.

Anyway, designing a trust model in VANETs is an interesting and challenge subject. It makes kinds of applications in VANETs more safe, reliable and convenient. It will also play an important role in the upcoming vehicle cloud computing.

References

[1] Ma, Junxia, and Chen Yang. A Trust-based Stable Routing Protocol in Vehicular ad-hoc Networks. International Journal of Security & Its Applications, 9(4), 2015:107-116

[2] Qin Li, Amizah Malip, Keith M. Martin, Siaw-Lynn Ng, Jie Zhang. A Reputation-Based Announcement Scheme for VANETs. IEEE Transactions on Vehicular Technology, 61(9), 2012: 4095-4108

[3] Xiaoqing Li,Jicheng Liu,Xuejun Li, Weiying Sun. RGTE: A Reputation-based Global Trust Establishment in VANETs.5th International Conference on Intelligent Networking and Collaborative Systems,2013,pp:210-214

[4]Audun Josang. The Beta Reputation System. 15th Bled Electronic Commerce Conference e-Reality: Constructing the e-Economy, Bled, Sovenia, 2002

[5] Yang, Nianhua. A Similarity based Trust and Reputation Management Framework for VANETs. International Journal of Future Generation Communication and Networking, 6(2),2013: 25-34.

[6] Zhen Huang, Sushmita Ruj, Marcos A. Cavenahi, Milos Stojmenovic, Amiya Nayak. A Scocial Network Approach to Trust Management in VANETs. Peer-to-Peer Networking and Applications, 7(3), 2014:229-242

[7] Wang, Guanghao, and Yue Wu. BIBRM: A Bayesian Inference Based Road Message Trust Model in Vehicular Ad Hoc Networks. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference, IEEE, 2014:481-486