Trust in Vehicle-to-Vehicle Communication

BoakyeDankwa[1], RaghavendranVijayan[2], DarshSanghavi[3], MihranTuceryan[4], Rajeev R. Raje[5]
[1,2,3,4,5]Department of Computer and Information Science
[1,2,3,4,5]Indiana University Purdue-University Indianapolis (IUPUI)
Indianapolis, Indiana, USA

***Abstract*—In traditional Pedestrian Automatic Emergency Braking (PAEB) system, vehicles equipped with onboard sensors such as radar, camera, and infrared detect pedestrians, alert the driver and/ or automatically take actions to prevent vehicle-pedestrian collision. In some situations, a vehicle may not be able to detect a pedestrian due to blind spots. Such a vehicle could benefit from the sensor data from neighboring vehicles in making such safety critical decisions. We propose a trust model for ensuring shared data are valid and trustworthy for use in making safety critical decisions. Simulation results of the proposed trust model show promise.**

***Index Terms*—Trust; Trust Model; Reputation**.

1. INTRODUCTION

In traditional Pedestrian Automatic Emergency Braking (PAEB) system, vehicles equipped with onboard sensors such as radar, camera, and infrared detect pedestrians, alert the driver and/ or automatically take actions to prevent vehicle-pedestrian collision. In some situations, such as shown in Figure 1, the sensors of the black sedan may not detect the pedestrian which could result in a crash. However, if the vehicles in the scenario shared sensor information in a vehicle-to-vehicle (V2V) communication fashion, such a crash can be avoided.

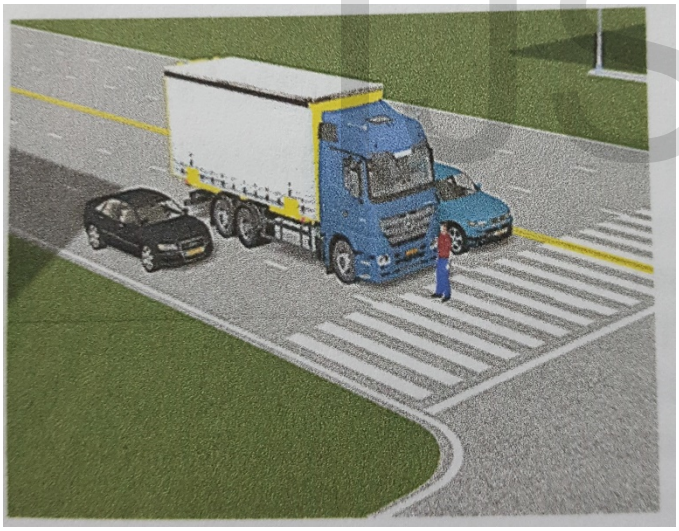


Fig. 1: Crash Scenario due to an obstruction in the middle (Courtesy: Dr. S. Chien, S. R. Bhatnagar and TASI Simulator)

In V2V communication, every transceiver device involved sends data such as pedestrian crossing, toll gate and accidents to other transceiver devices. Constraints such as the networkQuality of Service, the quality of vehicle sensors and the overall system directly impact the quality of the exchanged data. These messages are used in making critical decisions such as slowing down to avoid a collision with a pedestrian. As such, the validity of these messages play an important role in making safety critical decisions. For example, questions such as are the messages referring to the same pedestrian, or are they referring to an object by the roadside need to be addressed.

In this paper, we attempt to contribute to the area of V2V-PAEB research by focusing on trust in such a V2V-PAEB system. We propose a trust model to quantify trust for communications in a V2V-PAEB system. Our model filters incoming messages, evaluates trustworthiness and forwards the messages, along with their quantified trust data, for safety decisions to be made upstream. Our trust model can be seamlessly integrated with the Transportation Active Safety Institute (TASI) computer simulation at IUPUI TASI lab. Communications between the vehicles can be secured with appropriate authentication and encryption technologies recommended by Vehicular Ad hoc network (VANET) standardization bodies, therefore we assume the presence of secure communication channels between vehicles.

2. RELATED WORK

In [1], the authors present a reputation assisted trust management mechanism for VANET using trusted group formation. The formed group manager has the privilege to change the trust value of the vehicle dynamically based on its behavior in the network. Government vehicles are chosen to be the pre-trusted vehicles and they act as group manager. Vehicles securely form groups following a set of sequential steps: setup, join, sign, verify and open. The trust levels are of two types: static and dynamic reputation. Static trust increases/decreases based on the reputation of received messages, dynamic trust on the other hand, increases/decreases based on the source vehicle's behavior, and reputation of its messages received via other vehicles. The notion of a group manager implies that there must be a group manager present in any given time in order to establish a formation. This raises scalability issues. In our proposed system, each vehicle makes its own trust assessment rather than rely on a neighbor to make it for them.

Liao et. al. [2] propose a centralized trust management scheme based on incident reports. The central authority (such as a Regional Traffic Management Center) monitors all vehicles in the network for incident detection. Trust values areupdated based on incident, and periodically broadcasted to all vehicles. Messages received in V2V communications are vetted against these reports to determine their trustworthiness. The main drawback of this method is, it misses a dynamic real-time trust component. Although the incident reports contain reputation data, the coordinating vehicles are in a constant dynamic environment and

require a real-time evaluation of trust in addition to the reputation data. Our proposed system incorporates both real-time and reputation trust components to evaluate an aggregate trust.

The authors in [3] propose an announcement based scheme in which vehicles provide feedback to the messages received and build reputation score based on them. The system includes a reputation server which collects feedback and broadcasts reputation data on the network. This means that the vehicles which are not in close proximity with each other but within reach of the same reputation server would receive the broadcast, wasting storage space and bandwidth. Our system requests data on demand from a remote reputation server.

3. TRUST MANAGEMENT SYSTEM

Trust is a subjectiveconcept as indicated in [4]. It is a relationship existing between two participants. [5] defines trust as:

"Trust is the willingness of the trustor (evaluator) to take risk on a subjective belief that a trustee (evaluatee) will exhibit reliable behavior to maximize the trustors interest under uncertainty (e.g. ambiguity due to conflicting evidence and /or ignorance caused by complete lack of evidence) of a given situation based on the cognitive assessment of past experience with the trustee"

For example, in human associations, we trust other people based on our past experiences with them and we are able to rely on such experiences to believe that they will exhibit reliable behavior in unfamiliar or ambiguous situations. On the contrary, if we distrust someone, then we believe we cannot assume that they will exhibit reliable behavior under such conditions. It is important to note that trust is contextual and constantly evolving. For example, a trusted person can exhibit reliable behavior in one scenario but unreliable behavior in a different context (e.g. trusting Bob as a good math teacher, but a bad basketball player). Also if we have trusted Alice with a credit card and end up with unknown charges, our trust for her with respect to this context will reduce. It is in this context that we propose a trust model for the V2V application.

The authors of [6] describe a trust management system as a framework designed to help make better decisions based on trust information. As shown in Figure 2 they model trust management system as four interacting components: trust modeling, trust inference and trust decision, and the applicable context [6].
This (Figure 2) trust model deals with how to represent trust in computational models using available raw data.

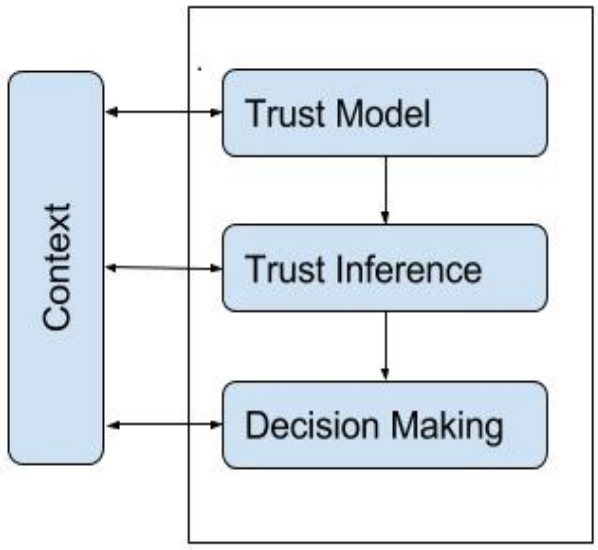


Fig. 2: Trust Management System (Redrawn from [6])

Discrete andcontinuous numerical valuesare usually usedto quantitatively measure trust in many applications [5]. Sometimes there is the need to aggregate trust from various participants in order to infer trust between two parties. There are two important operators in trust reference schemes: transitivity operator and aggregation operator [7]. Transitivity operator is used to calculate trust propagation in a single chain. Aggregation operator on the other hand, is used for combining parallel trust paths between the truster and the trustee in the case where there exist more than one trust path between them [8].

The last component of the trust model is decision making. This is where a decision is made based on the evaluated trust between the truster and the trustee.

4. PROPOSED TRUST MANAGEMENT SYSTEM FORV2V-PAEB

We model trust as a continuous numerical value in the range [0 1]. Zero (0) represents complete distrust and one (1) represents complete trust. We compute a trust value for each sensor data received in messages from neighboring vehicles. Each message contains one or more sensor data. There are three trust components involved, we call these, measured trust, short-term reputation, and long-term reputation as shown in Figure 4. These three components are then aggregated to achieve the resultant trust used in the V2V-PAEB decision logic. Figure 3 shows the data flow relationship between our trust model and the TASI V2V-PAEB simulation environment. Messages from the environmental model are processed by the transformation model which transforms all sensor values onto a common reference frame. Our trust model then computes a trust value for each message and forwards the messages, along with their quantified trust data, for safety decisions to be made by the V2V-PAEB control model.

1) *Measured Trust:* We compute this trust value in two

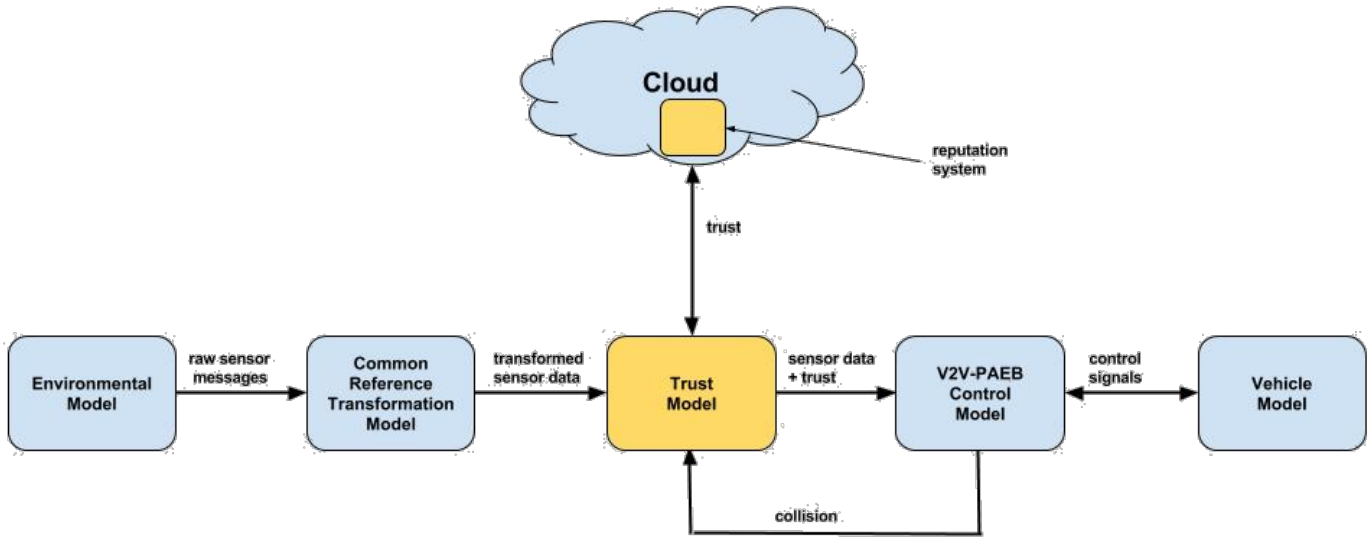


Fig. 3: TASI V2V-PAEB Simulation System with Trust Management

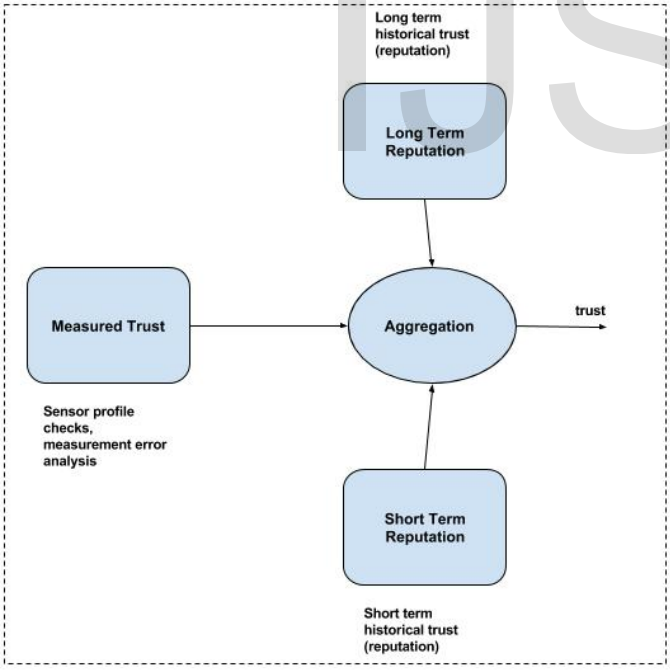


Fig. 4: Proposed Trust Model for V2V-PAEB

parts, first a value based on a known sensor profile, and thena value based on the error probability in the measured raw data. This model is contextual and dependent on the type of sensor and quantity being measured. For example, a typical profile for a sensor that measures a pedestrian's position would include reasonable lower and upper limits in the measured value. A lower limit can be selected as zero feet from the subject vehicle in the same plane as the direction of travel. An upper limit can also be selected as 'x' feet (based on the speed of the subject vehicle) in the same plane as the direction of travel. A value outside this range, for example, positiondata which indicates a pedestrian above or below the plane of travel would suggest a failed sensor and hence, be deemed untrustworthy and therefore, not considered in making control decisions. This serves to filter out outliers from the analysis. In a rare situation where all messages are declared failed, it will be up to the V2V-PAEB control logic to decide which safety action to take. Each sensor can have as many profiles as can be constructed. The other part of the measured trust is based on measurement error in the physical quantity. Heuristic models such as Bayesian point-estimation techniques can be used to estimate the error involved in measurements. The results of these analyses are then be mapped onto a trust plane.

2) *Short Term Reputation:* Here we maintain a local historical trust value for each vehicle we receive messages from. If a message is not received from a given vehicle after some predefined time, for example if it is no longer within range, it is dropped from this historical list. Each trust value is based on short-term history of decisions made by the V2V-PAEB control logic. This requires feedback from the V2V-PAEB control logic. For this to be feasible, the V2V-PAEB control system must be able to perform an inverse operation to map the output decision back onto the contributing vehicles. This inverse operation is problematic since the consequence of the control decision is binary (collision, or no collision). Therefore, we adopted a simpler universal approach where the short-term trust values of all involving vehicles are penalized (i.e., assigned a default reset value) when a collision results from a control decision. On the

other hand, when collision is avoided, all involving vehicles are rewarded with a boost in their short-term trust values (i.e., trust values incremented by a fixed amount). The reward value depends on the minimum number of in-profile messages that must be received in order for a message to achieve its full trust potential. Sample selection of penalty and reward values will be described inSection V. This trust component is periodically uploaded remotely to update a long-term reputation.

3) *Long Term Reputation:* Vehicles equipped with a V2V-PAEB system would periodically establish a secure connection with a reputation server (via LTE/4G/5G) in the cloud, and upload short term reputation trust values. These historical trust data would be used to estimate a reputation value for each kind of vehicle.

4) *Trust Aggregation:* The three trust components are then aggregated to provide a single trust value for each sensor value used for decision making. We adopted a simple weighted additive aggregation scheme.

V. IMPLEMENTATION DETAILS

For simplicity, pedestrian position data from a single sensor is considered for demonstration purposes. A simple range-check is used as a profile for the sensor (in a real-world application, there would be various data from different sensor sources, that would require different sensor profiles) that is, the Euclidean norm of each sensor value from each vehicle must fall within a certain reasonable range to be deemed trust-worthy. When a sensor values falls outside the accept-able range, it is marked as untrustworthy and automatically assigned a trust value of 0. When a signal falls within the profile, it moves on to the error analysis. Here, we used the Euclidean distance from the mean of the signals as an error measure. That is, the farther away from the mean, the less trust we assign to the signal, the closer it is, the more we trust the signal. We assign a trust value of 1 to the mean, and 0.5 to the signal farthest away from the mean. Note that 0.5 is the default trust assigned to each signal that falls within the profile. We linearly interpolate any trust values in-between these two limits.

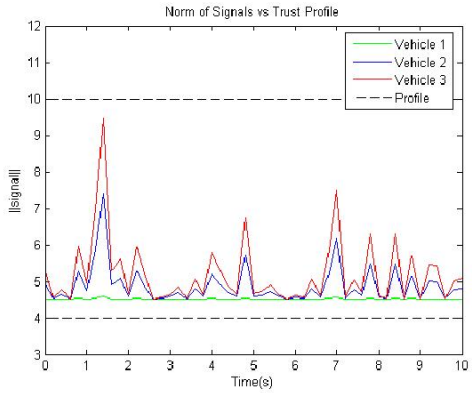
A short-term reputation model models the interactions be-tween the output of the V2V-PAEB simulation and the trust model. If a control decision does not result in a vehicle-pedestrian collision, the trust value for all vehicles involved is increased by a small value (0.1), i.e., five in-profile messages must be received from a particular sensor to achieve its maximum short-term reputation value (0.5). If a collision resulted from a control decision, all vehicles get a default short-term reputation value of zero.

A fixed trust value of 0.5 was assigned as long-term reputation trust value for all messages. A more complex long-term reputation model will be implemented as a future extension.

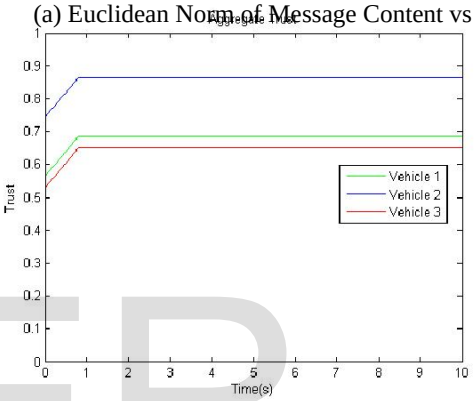
The trust values from all there models are weighted and aggregated into a single trust value to be sent to the V2V-PAEB simulation control model.

VI. RESULTS AND DISCUSSIONS

The simulation consists of messages from three vehicles. For demonstration purposes, only a single sensor type was used. This could be say, the position of velocity of a pedestrian as measured by each vehicle. The signals used in the trust



(a) Euclidean Norm of Message Content vs Time



(b) Aggregate Trust vs Time

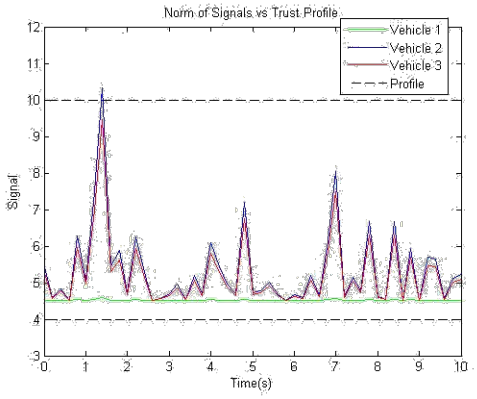
Fig. 5: Aggregate Trust for In-Profile Messages

analysis are assumed to have been transformed to acommonreference by the TASI simulation environment downstream of the trust model as described in Section IV.

Figure 5 shows the nominal case where each of the messages fall within profile. That is, messages received by the subject vehicle from its neighbors contain sensor data whose Euclidean norm falls within the measured quantity's predefined profile (lower and upper bounds) as shown in Figure 5(a). All the messages passed the profile check and therefore are used in the signal estimation. The result shows an aggregate trust values which convergence for all three messages after a few seconds as shown in Figure 5(b). The trust value of each message depends on how far the content of each individual message deviates from the estimated mean of the contents of all three messages.

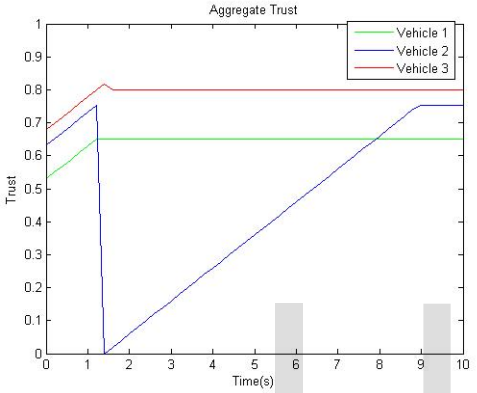
The second result, Figure 6, shows the behavior of aggregate trust when a message fails the profile check. The Euclidean norm of the data in message (vehicle 2), Figure 6, at time t = 1.4s exceeded the upper limit of the profile. This resulted in that particular message being dropped from further analysis downstream. It can be observed that its aggregate trust value drops to zero (distrust) following an

(a) Euclidean Norm of Message Content vs Time



(b) Aggregate Trust vs Time

Fig. 6: Aggregate Trust for Out-of-Profile Message



out of profile event. This is a desired behavior since it essentially filters out outliers from the trust analysis.

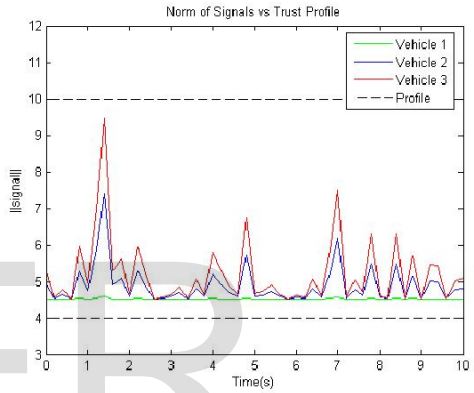
If the signal falls back in-profile,its aggregate trust value gradually increases and settles if it stays in-profile. That is, we have to be cautious not to trust a particular sensor immediately following an out-of-profile event since that's usually an indication of a degraded sensor and a precursor to complete sensor failure.

The final result shows how the aggregate trust of all in-profile contributing messages would behave after a collision event. Figure 7 shows that the aggregate trust value for all messages falls to a predefined penalized default value following a collision event at time t = 0.8s. The significance of this scenario is that it penalizes the reputation of all contributing vehicles and their short-term and long-term reputation would be updated with lower trust values following a collision event.

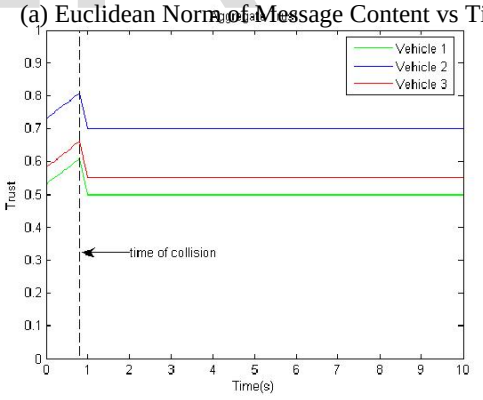
VII. CONCLUSIONS AND FUTURE EXTENSIONS

We have proposed a trust model which estimates trust in V2V-PAEB communications. Sensor profiles are used to screen messages from inclusion in safety decisions. Error probability models are used to estimate signal error and assign trust accordingly (measured trust), which is aggregated with a short-term reputation and long-term reputation to get an aggregate trust for use in V2V-PAEB control logic.

This work is an early attempt to solving the trust problem in V2V-PAEB communications. Integrating this model with theTASI simulation environment would be helpful in determining the performance of this model. Future work would involve refinements such as using robust estimation techniques for sensor profile checking, and modeling profiles for complex sensors. The detailed workings of the long-term reputation model is also left as a future task.



(a) Euclidean Norm of Message Content vs Time



(b) Aggregate Trust vs Time

Fig. 7: Aggregate Trust for a Collision Event

ACKNOWLEDGMENT

The authors would like to thank Dr. S. Chien and S. R. Bhatnagar of the Department of Electrical and Computer Engineering at IUPUI, and TASI for granting us access to the TASI simulator.

REFERENCES

[1] S. V. B. K. Chaurasia, "Trust based group formation in

vanet," in Modern Traffic and Transportation Engineering Research, April 2013, pp. 121– 125.

[2] C. Liao, J. Chang, I. Lee, and K. K. Venkatasubramanian, "A trust model for vehicular network-based incident reports," in 2013 IEEE 5th International Symposium on Wireless Vehicular Communications (WiVeC), June 2013, pp. 1–5.

[3] Q. Li, A. Malip, K. M. Martin, S. L. Ng, and J. Zhang, "A reputation-based announcement scheme for vanets," IEEE Transactions on Vehicular Technology, vol. 61, no. 9, pp. 4095–4108, Nov 2012.

[4] L.Gallege, D. Gamage, J. Hill, and R. Raje, "Understanding the trust of software – intensive distributed systems concurrency and computation:' practice and experience," vol. 28, no. 1, pp. 114-143, .2016.

[5] J. H. Cho, K. Chan, and S. Adali, "A survey on trust modeling," ACM Comput. Surv., vol. 48, no. 2, pp. 28:1-28:40, Oct. 2015. [Online]. Available: http://doi.acm.org/10.1145/2815595

[6] J. Sabater and C. Sierra, "Review on computational trust and reputation models," Artificial Intelligence Review, vol. 24, no. 1, pp. 33-60, 2005. [Online]. Available: http://dx.doi.org/10.1007/s10462-004-0041-5

[7] Y. Wang and M. P. Singh, "Trust representation and aggregation in a distributed agent system, "in Proceedings of 21st National Conference on Artificial Intelligence – Volume 2, ser. AAAI'06. AAAI Press, 2006, pp. 1425-1430. [Online]. Available: http://dl.acm.org/citation.cfm?id=1597348.1597415

[8] A. Jøsang, "A logic for uncertain probabilities," Int. J. Uncertain. Fuzziness Knowl.-Based Syst., vol. 9, no. 3, pp. 279–311, Jun. 2001.[Online]. Available: http://dx.doi.org/10.1142/S0218488501000831