A distributed advanced analytical trust model for VANETs

Gazdar Tahani, Abderrezak Rachedi, Abderrahim Benslimane, Belghith Abdelfettah

A Distributed Advanced Analytical Trust Model for VANETs

Tahani Gazdar*‡, Abderrezak Rachedi†, Abderrahim Benslimane* and Abdelfettah Belghith‡
*University of Avignon, France
Email: tahani.gazdar@alumni.univ-avignon.fr, abderrahim.benslimane@univ-avignon.fr
†University of Paris-Est Marne la Vallée, France
Email: rachedi@univ-mlv.fr
‡University of Manouba, Tunisia
Email: abdelfettah.belghith@hotmail.com

***Abstract*—In this paper we propose a trust model based on a Markov chain in order to formalize the trust metric variation and its stability in the context of Vehicular Ad hoc Networks (VANETs). The proposed model takes into account not only the dynamic trust metric variation according to the vehicles behaviors, but also the constraints related to the monitoring process. In our model each vehicle can act as monitor and update the trust metric of its neighbors according to their behavior in the network. In addition, our model can be customized through different parameters like the trust interval and the number of transitions needed to reach the highest trust level. This flexibility enables to adapt the model according to the application context. The performance evaluation of the proposed model is presented with different parameters and two types of disruptive vehicles are taken into account: malicious and selfish. The obtained results show the resistance, the robustness and the incentive of the proposed model against the fluctuations of the vehicles behaviors.**

I. Introduction

In vehicular environments, the time to react to a given situation is very critical and a vehicle must be able to accurately check the trust of the received information in real time. The trust and reputation models [1] are proposed as new approaches to circumvent with this constraint and to filter out inaccurate messages and malicious vehicles. Trust establishment is tagged in many existing research works for peer to peer, sensors, and mobile ad hoc networks [1] [2]. However, in vehicular environments it is facing tremendous specific challenges related to their characteristics. In general vehicular networks do not have any centralized third party. The only possible communications with infrastructures take place with Road Side Units (RSUs) which are not deployed along the roads. Therefore, centralized systems are not suitable to establish trust in vehicular environments. Furthermore, the vehicles are traveling with a high speed, consequently, the communications between the vehicles are short in time and it is difficult to form an experience history between peers. In addition, a trust model must be scalable providing the same achievement independently on the density of vehicles in the network.

The main existing trust models for VANETs are based on the verification of vehicles identities and their legitimacy in the network [3], [4], [5]. They are classified as entity oriented models such as identity-based systems where the trust metric is related to the vehicle credentials and its trustworthiness is static. Other existing trust models are based on a data-oriented approach. Indeed, in VANETs, when the vehicle introduces a new information in the network it will be responsible for the consequences of this information. In this paper, we propose a new hybrid dynamic trust model combining both approaches: entity and data oriented. We use a Markov Chain to formalize the proposed trust model. The goal of this modeling is to take into account different parameters related to the robustness, stability and flexibility of the trust model. Unlike static trust models, we propose a dynamic model based on the monitoring of the instantaneous vehicles behaviors in the network. The monitoring process considers the legitimacy of the information and the cooperation rate of the vehicles. We include also the constraints related to the efficiency of the monitoring process, particularly, the probability of false positives and negatives. Furthermore, our model is fully distributed, the assessment of vehicles behavior does not require any type of infrastructure.

The remainder of the paper is organized as follows. First, we discuss some existing trust models designed for VANETs. In section 2, we detail the proposed trust model. Section 3 exposes the simulation results and section 4 concludes the paper.

II. Related work

The trust models in VANETs can be classified into three main types: entity-oriented, data-oriented and hybrid models. In the entity-oriented trust models the evaluation of the legitimacy of an entity is required. In [5], the authors propose a reputation-based trust model where the vehicles are organized off-line into groups and each one has a reputation value. Each group reputation increases if the average of its members opinion is conform to the road state. It is obvious that this approach is not resilient against colluding vehicles which belong to the same group and they broadcast false information to make the reputation score of their group drive down. Another shortcoming is the absence of a reputation value for each vehicle to punish malicious ones. In our proposal, we remedy to this problem by an instantaneous evaluation of the vehicles behavior and a malicious vehicle is revoked whenever

it is detected. In [4], the authors propose a fuzzy approach to decide whether to accept a warning message or not based on the trustworthiness of the issuer of the message. In this model, the authors assume that a vehicle requests from its neighbors information about the reputation of its peers which makes a supplementary overhead also this needs additional time. However, in our proposal each vehicle executes a stand-alone trust metric evaluation process using the already existing messages in the network. In the above exposed models, the trust establishment is related to the verification of the trustworthiness of the entities. However, inaccurate information cannot be detected without verifying the information itself.

Many research works propose instead, data-oriented trust models which require the evaluation of the trustworthiness of the information received in the messages. The authors in [6] propose a data trust model where the validity of the received reports about occurred events is inferred by a decision module [7] [8] to calculate the posteriori probability of the events. However, since inference module use the prior probability, it is not easy to derive it since the high speed. The authors in [9] proposed an event-based reputation model to filter out bogus messages. In order to decide about the legitimacy of the messages, the vehicle observes if the behavior of the reporter corresponds to the standard behavior result of that event. We notice that this solution is not realistic because a malicious vehicle can broadcast a message about an unreal event and it reacts correspondingly. Nevertheless, data oriented models seems to be efficient to filter out malicious data that is why we build our model on. Additionally, we combine it with a cooperation assessment parameter.

In order to circumvent the shortcoming of the two above mentioned approaches, the authors proposed in [10], a hybrid approach using a piggybacking technique. In fact, a trustworthiness opinion is appended to each message reporting an event. The drawback of this proposal is that the first opinion appended to the message will affect other opinions since its computing is recursive; it is based on opinion received in the message. In [12], the authors assume that in the network there is a set of trusted vehicles called anchors which broadcast reliable data. The data validation is ensured either by comparing the received data to other vehicles agreement or to the data of the anchors. The shortcoming of this model is that the validation process is accurate only if there is a sufficient number of reports from other vehicles. The trust model that we propose is a fully distributed and hybrid approach based on a monitoring process. We aim to conceive a flexible model combining many parameters relayed to the cooperativeness of vehicles in order to detect selfish ones, their ability to broadcast and forward legitimate information and the efficiency of the monitoring process.

III. The Analytical Trust Model

In this section, we describe our proposed trust model. We present the states transitions diagram for the Markov chain model. The model resolution, also the computation of different transition probabilities are detailed.

A. Trust Model Overview

In the network, we consider that when an event occurs on the road, all vehicles which are in the vicinity of that event must broadcast alerts messages reporting it. Furthermore, vehicles forward all received messages from their neighbors. We note that the arrival of alert messages to the transmission queue of vehicles is modeled in the following section.
Our purpose is to establish a dynamic and distributed trust model where each vehicle called *monitor* affects a local trust metric T_m to each vehicle from its neighbors called *monitored* vehicle. In fact, the evaluation of the behavior of the monitored vehicle by the monitor vehicle is based on two main aspects: the reliability of the message sent by the monitored vehicle and its cooperation ratio. Thus, according to the outcome of the monitoring process, the monitored vehicle will have its T_m increased, decreased or unchanged. Additionally , the T_m can change to null, and as presented in figure 1, this transition is weighted by a probability related to the honesty of the monitored vehicle when it broadcasts the alert messages, also it depends on the current state of the vehicle.

We model the update process of the T_m at the monitor vehicle using a discrete-time Markov chain with $N+1$ states and a transition matrix $P = (P_{i,j}(t))_{0 \leq i,j \leq N}$ as represented in figure 1. Consider a random variable $(X_t)_{t \geq 0}$ which represents the current local T_m corresponding to a given state of a monitored vehicle assigned by a monitor vehicle, the probability of transition from state i to state j is:

$$P_{i,j}(t) = Pr(X_t = j | X_{t-1} = i) \tag{1}$$

The T_m has a value in $[0, 1]$, state 0 is the non trusted state wherein $T_m = 0$ and state N is the highest trusted state where $T_m = 1$. Each vehicle has an initial trust metric T_0 in $[0, 1]$. The interval $[0, 1]$ is divided into $N + 1$ states, each one represents a step of γ (1 mod $\gamma = 0$). The values of γ and N are determined based on the degree of accuracy assessment and severity towards the T_m of vehicles that we want to achieve with our model. By using these two parameters we aim to make our model flexible in the context wherein it is used.

B. States Transition Probabilities

1) One step increasing/decreasing of the T_m: If the current state is i at time t ($Pr(X_t = i) > 0$) and the vehicle shows a positive behavior, its T_m transits to the state $i+1$ otherwise it transits to the state $i-1$. The positive behavior in our model is related to: the ability of the vehicle to correctly forward all received legitimate messages, and to the legitimacy of its own broadcasted messages. The transitions probabilities are expressed as follows:

$$\begin{aligned} P_{i,i+1}(t) &= p_i(t-1) * p_c * p_w & 0 \leq i < N \\ P_{i,i-1}(t) &= p_i(t-1) * (1 - p_c) * p_w & 0 < i \leq N \end{aligned} \tag{2}$$

Where $p_i(t)$ is the probability to be in state i at time t, given that the initial state is 1, p_c is the probability to positively cooperate in the network, and p_w is he probability to correctly evaluate the received messages. It is expressed as follows:

$$p_w = 1 - p_e \tag{3}$$

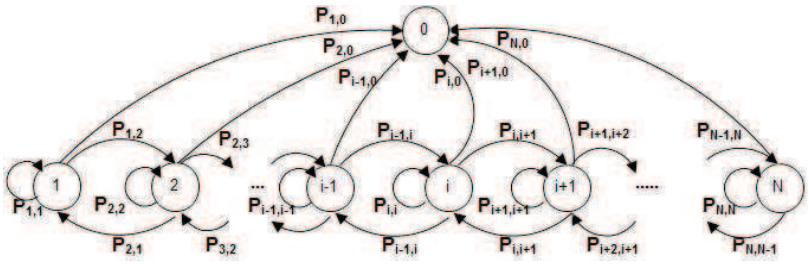


Fig. 1. States transitions diagram of the proposed approach

In equation 3, p_e is the probability of false positives and false negatives following the monitoring process [13]. Using this parameter, we aim to take into account the constraints related to the nature of the network and to the monitoring in wireless environments. Indeed, this avoids the over and under estimation in the monitoring and consequently in the trust level evaluation. Particularly, p_e includes the probability of collusion while transmitting warning messages and the failure of the monitored vehicle to access to the transmission channel.

From the transition matrix P, it is possible to compute the probability to be in state i at time t, $p_i(t)$. In fact, given that the initial state of a vehicle is $X_0 = 1$, the probability for our Markovian process to be in state k at time $t_k > 0$ is $p_k(t_k) = P_{1,k}(t_k)$. In addition, the probability to reach state i at time $t > t_k$ given that $X_{t_k} = k$ is $P_{k,i}(t)$. Therefore, we can use the Chapman-Kolmogorov equation [11] to compute the probability $p_i(t)$ that a vehicle is in state i at time t:

$$p_i(t) = \sum_{k \ in \ [1..N]} P_{1,k}(t_k) * P_{k,i}(t) \tag{4}$$

In order to evaluate the cooperation of a monitored vehicle, first, a monitor vehicle calculates a forwarding rate called F. The forwarding rate F is the number of messages forwarded by a monitored vehicle divided by the total number of messages transmitted by the monitor vehicle:

$$F = \frac{the \ number \ of \ forwarded \ messages}{the \ total \ number \ of \ transmitted \ messages} \tag{5}$$

Secondly, the monitor vehicle calculates the probability that the monitored vehicle has a positive cooperation in the network denoted p_c as follows:

$$p_c = F * P_m \tag{6}$$

where P_m is the probability that the monitored vehicle is not malicious. In fact we use this parameter in order to evaluate the honesty of the vehicle when transmitting or forwarding information. Tremendous works exist in the literature aiming to detect malicious nodes in MANETs [14], [13]and VANETs [4].

2) State sojourn probability : A vehicle can keep the same T_m for a certain period of time because either it has no message in its buffer to forward or it has not detected events on the road. We consider that the application layer in the monitored vehicle generates alert messages according to a Poisson process with a rate λ_1. In addition, the monitored vehicle receives alert messages from other vehicles according to a Poisson process with a rate $\lambda_2 \geq \lambda_1$. We suppose that a message needs the period t_s to be treated in the higher layer before being sent, so we assume that the time required for the treatment of messages is exponential with a rate $1/t_s$. Then, according to [16], the probability P_q that the transmission queue is empty is:

$$P_q = 1 - \frac{1 - (1-\theta)\theta^B}{1 - \theta^{(B+1)}} \tag{7}$$

$$\theta = (\lambda_1 + \lambda_2) * t_s \tag{8}$$

Where B is the size of the transmission queue and we assume that λ_1,λ_2 and t_s have the same values for all vehicles. Thus, from equation 7 we deduce the probability that a node sojourns in state i, $P_{i,i}$ $(i \neq N)$:

$$P_{i,i}(t) = p_i(t-1) * P_q \tag{9}$$

3) Trusted state sojourn Probability: The vehicle keeps the trusted state N ($T_m = 1$) either because it positively cooperates as discussed above or it has no messages in its transmission queue. We express $P_{N,N}$ the probability to sojourn in state N as follows:

$$P_{N,N}(t) = p_N(t-1) * (p_c * p_w + P_q) \tag{10}$$

Yet, the trusted vehicles are also monitored by their neighbors in order to avoid that they benefit from the trusted state and behave maliciously or selfishly in the network.

4) Transition to the non trusted state: As we mentioned above, the monitor vehicle assesses both the cooperativeness of the monitored vehicle and the legitimacy of the information it broadcasts. Thus, according to the outcome of the monitoring process, the T_m of the monitored vehicle can nullify with a given probability that reflects the legitimacy of its broadcasted messages. The probability of this transition is related to the current state of the vehicle and to its honesty represented by P_m. Logically, if a vehicle reaches a high T_m, this means that it is almost honest as expressed by equation (6). However, a malicious vehicle can behave honestly to reach the highest trust level and then it tries to benefit from its state and to broadcast false information. Thus, we consider this transition in order to detect such a malicious behavior

known as camouflage attack. The probability that the vehicle transits to state 0 is calculated as follows:

$$p_{i,0}(t) = p_i(t-1) * (1 - P_m) \quad (11)$$

IV. Performance Evaluation

A. Analytical Results

In order to validate our trust model we consider a Markov chain as represented in figure 1 with $N = 10$ states. Each one represents a step $\gamma = 0.1$. The initial trust metric for each vehicle is $T_m = 0.1$. We conducted a set of preliminary tests in order to investigate the convergence and the persistence of the proposed approach as function of different parameters. Furthermore, we study the resilience of the model against some misbehaving scenarios.

1) Convergence of the T_m: We investigate the convergence of our model, particularly we are interested on the required time and the needed conditions for a vehicle to reach the trusted state where T_m=1 and to remain in. To this end, we plot the probability to get $T_m = 1$ that we call the trustworthiness of a vehicle, as function of the time, the forwarding rate F and P_m. We set parameters p_e to 0.20 as computed in [13] and P_q to 0.25.

We notice from figures 2a and 2b that for time units less than 10, $P(T_m = 1)$ is equal to 0 because a vehicle starts from $T_m = 0.1$ and it must pass by all states from 1 to $N = 10$, then the vehicle needs at least 10 time units to reach $T_m = 1$. After, the $P(T_m = 1)$ incessantly grows until reaching a maximum in the 14^{th} time unit. Regarding the attenuation of $P(T_m = 1)$ after reaching the maximum in figure 2a, we explain this behavior by the cumulating effect of P_m. If the vehicle does not improve its behavior related to P_m, the probability to reach $T_m = 1$ decreases. However, in figure 2b where $P_m = 1$, when $P(T_m = 1)$ reaches 1 it does not attenuate as for the previous case where $P_m < 1$. This result confirms our explanation for the attenuation in the previous plot, also this result points out the sensibility of the trustworthiness to the parameter P_m. In addition, we remark in both plots that for small values of F (0.35 and 0.45) the drop of $P(T_m = 1)$ is less rapid compared to higher values of F (0.90 and 1.00), however it is obvious that $P(T_m = 1)$ is less important. Hence, if a vehicle reaches the trusted state with a legal behavior and a full cooperation, it keeps its trust state.

We conclude that the trustworthiness is getting higher for high values of the forwarding rate F. However, the persistence in the trusted state strongly depends on the behavior of the vehicle expressed by P_m. The more positively the vehicle cooperates, the more chance it has to be trusted, and the longer it keeps its trusted state.

2) Impact of a disruptive behavior: Let us now study the ability of our trust model to handle dynamic behaviors of the vehicles. In general, a disruptive vehicle divides its behavior into two parts: in the first part it positively participates in the network in order to reach the highest trust level. However, in the second part it changes its positive behavior to negative one in order to benefit from the reached trust level to attack the network. In this study, we focus on two main scenarios.

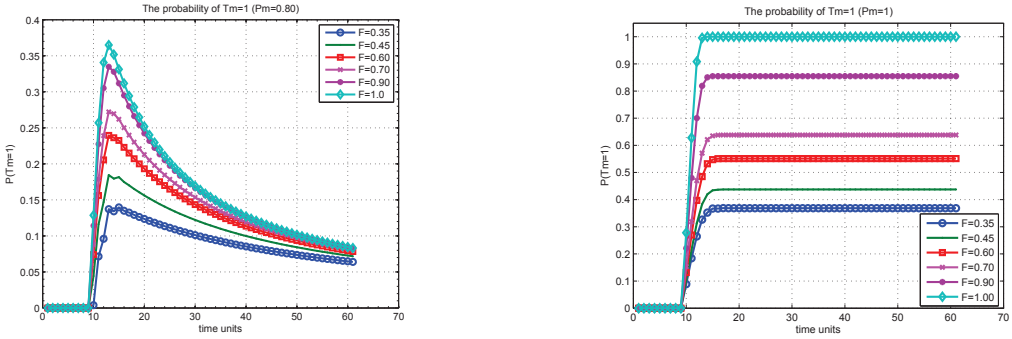
Scenario 1: : When a vehicle reaches the highest trust level, it will act selfishly by reducing its forwarding rate F in order to keep its throughput only for its own data transmission. The vehicle shows a good behavior (P_m=1 and F=1) for the first 20 time units to build up its T_m. Then it proceeds with a disruptive behavior following a pattern of bad behavior where it degrades its forwarding rate for 10 time units followed by a good behavior for 10 time units and so on. From the plot of figure 3, we notice that P(T_m=1) brutally decreases with the first misbehave time unit (21^{th}). Along the period the vehicle does not cooperate, its trustworthiness grows slowly because it is not acting maliciously in the network and it continues to transmits its own messages ($\lambda_1 \neq 0$). Once the monitored vehicle restores its cooperation rate, its trustworthiness resumes to the old value. We remark also that when the degradation decreases, the vehicle finds its previous trustworthiness level more rapidly. The difference in the fall of the trustworthiness between the curves proves that the trustworthiness of the vehicles strongly depends on its cooperation quality (p_c). This result proves that our model reacts rapidly and accurately to the change in the behavior of vehicles. It points out that our trust model is dynamic unlike static models where the trustworthiness is not sensible to behavior changes.

Scenario 2: : We consider a disruptive vehicle which shows a good behavior (P_m=1) for the first 20 times units to build up its T_m and then it proceeds with a disruptive behavior with P_m=0.45 as plotted in figure 4, giving a pattern of a bad behavior for 10 times units followed by a good behavior for 10 time units and so on. From the plot of figure 4, the trustworthiness decreases at the first misbehaving time unit. Once again, we notice the high sensibility of the proposed model to the parameter P_m which reflects the honesty of the vehicles. When the vehicle resumes its good behavior ($P_m = 1$), it doesn't restore its first trusted state and its trustworthiness increases slightly up to only 0.18 in figure 4. The same behavior of curves is repeated for the following steps until time unit 80.

There are two conclusions that can be derived from analyzing the results. First, if a vehicle proves a malicious behavior even for a short period of time, this affects its trustworthiness on the network and it is difficult to restore the trusted state. Secondly, we deduce that the proposed model is incentive. Indeed, the vehicle must be neither selfish nor malicious not only to reach the trusted state but also to remain in.

B. Simulation Results

We study in this section, the feasibility of our trust model in high mobility environments. Specifically, we investigate the convergence of the trust metric in such environments and we focus on the followed reasoning to decide different parameters used in our proposed trust model particularly, the number of states N and transition step γ. To this end, we conducted a set of tests using the simulator Veins [15] considering two



(a) $P_m = 0.80$ (b) $P_m = 1.0$

Fig. 2. The trustworthiness of the vehicle versus the time with different P_m

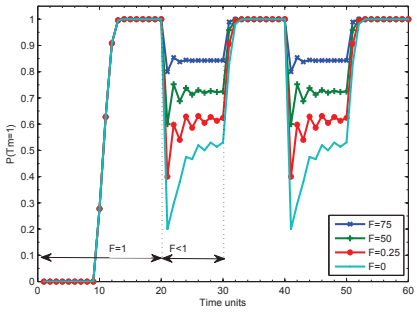


Fig. 3. Model reaction face to a disruptive behavior -Scenario 1, $P_m = 1$

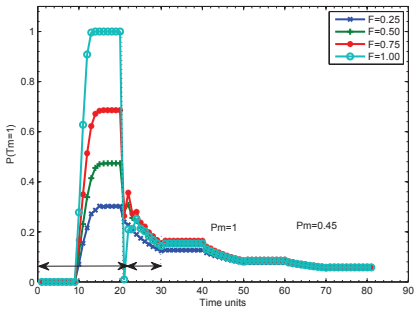
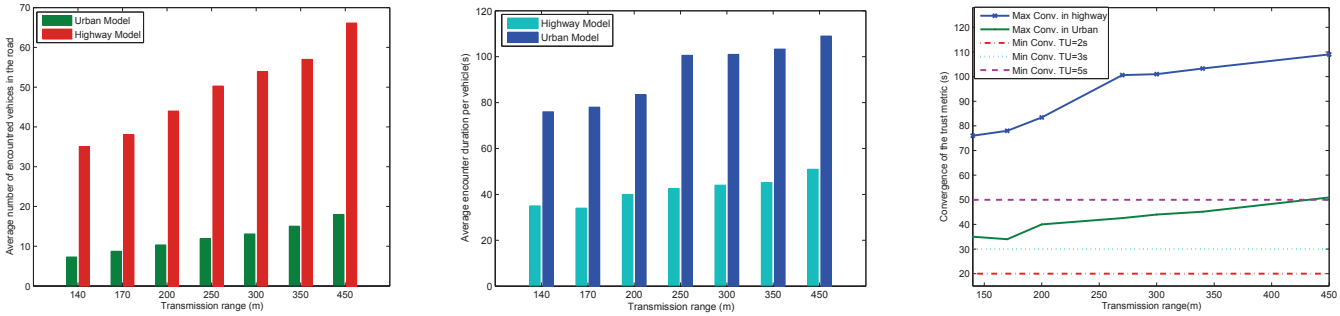


Fig. 4. Model reaction face to a disruptive behavior -Scenario 2

vehicular models: a Urban model and a highway. Vehicles travel with a maximum speed of $15m/s$ and $25m/s$ for the urban model and the highway, respectively. In the highway model, all vehicles are traveling towards the same direction. However, in the urban model the vehicles passes by multiple crosses and they can change the direction at any time there are in a cross. The arrival of vehicles in the road is a Poisson process with a rate of 2 vehicles per one second.

We plot in figures 5a and 5b the average number of vehicles encountered along a trip per one vehicle and the average encounter duration between two vehicles. From figure 5a, we remark that in the highway model, the average number of encountered vehicles is more important than the urban model. This is essentially due to the high speed of vehicles which makes the neighborhood change frequently in highway compared to the urban model. This is an important recommendation for our trust model. In fact, a vehicle will not travel isolated in the network and this augments the likelihood that its behavior is monitored.

According to the proposed model, the trust metric is evaluated each time the monitor receives a message from the monitored vehicle. Thus the time units expected in figures 2a and 2b correspond to the average time period between two evaluations of the trusted metric that we call $iteration\ duration$. It relies on the inter arrivals time of the messages from the monitored to the monitor and the average time required to assess F and p_c by the monitor vehicle. Hence, if the vehicle proves a legitimate behavior ($F = 1$ and $P_m = 1$), it needs only a time period of N*$iteration\ duration$ to have its $T_m = 1$. It is the minimal required convergence time of the trust metric. From figure 5b, the average encounter duration in the highway model is higher than urban model, it reaches $100s$. However, in the urban model, the average encounter duration is less than 60s. We plot in figure 5c, the maximal and minimal time for the trust metric convergence for both urban and highway model. For the minimal convergence time we consider different $iteration\ duration$: 2s, 3s and 5s and N=10 states. The goal is to investigate if the average encounter duration guarantees the convergence of the trust metric to the trusted state. As depicted in figure 5c, we remark that the maximal encounter duration in the urban model insures the convergence for N=10, only for $iteration\ duration < 5s$. We deduce that in case where the network traffic is reduced in the urban model, the number of states N can be reduced to quickly reach the convergence to the trusted state. However, we remark that for the highway scenario, the encounter duration guarantees the convergence even for limited traffic of messages. Hence, in this model our trust model can be executed with N higher than 10 states. Thus, from the analysis of above results, we conclude that our model is highly adaptive to applications. Indeed, the different parameters values are constrained by the



(a) The average number of encountered vehicles (b) The average encounter duration per one vehicle (c) The convergence of the trust metric

Fig. 5. The average number of encountered vehicles, the average encounter duration and the convergence of the T_m in highway and urban models

context where the trust model is processed, particularly the speed, the duration of encounter between vehicles and the network traffic.

V. Conclusion

In this paper, we propose a dynamic and distributed trust model aiming at establishing a trust relationship between vehicles and filtering out malicious and selfish vehicles. This trust model is formalized by Markov chain used to stress the trust evolution system, to introduce different parameters and to make it flexible. The monitoring process is based on the assessment of the cooperativeness of a vehicle also its honesty while broadcasting alert messages. In addition, the proposed model has a set of characteristics. It is incentive because it incites the vehicles to positively act in the network without adopting the selfish or the malicious behaviors in order to keep their reached trust level. It is robust because it is able to detect the different malicious behaviors. It is flexible because it presents different customized parameters like the trust interval and the number of transitions needed to reach the highest trust level. We conducted a set of simulations to investigate the performances of our trust model and to point out the reaction of our model to behavior changes. The obtained results illustrate the positive reaction of the model face to disruptive behaviors. In our future work, we are aiming at enhancing the performance evaluation of our trust model in real context of VANETs and we will extend our model in order to manage global trust metric where each vehicle has only one T_m known by all its neighbors.

References

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

[2] F. Marmol, J. Blazquez, G. Perez, *LFTM, linguistic fuzzy trust mechanism for distributed networks*, Concurrency and Computation: Practice and Experience, August 2011.

[3] D. Huang, X. Hong, M. Gerla, *Situation-Aware Trust Architecture for Vehicular Networks*, IEEE Communications Magazine, Volume 48, pages 128 - 135, November 2010.

[4] F. Marmol, G. Perez, *TRIP: a trust and reputation infrastructure-based proposal for vehicular ad hoc networks*, Journal of Network and Computer Applications, March 2011.

[5] A. Tajeddine, A. Kayssi, A. Chehab, *A Privacy-Preserving Trust Model for VANETs*, International Conference on Computer and Information Technology, China 2010.

[6] M. Raya, P. Papadimitratos, V. Gligor, J. Hubaux, *On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks*, IEEE Infocom 2008, Phoenix, AZ, USA 2008.

[7] T. M. Chen, V. Venkataramanan, *Dempster-Shafer Theory for intrusion detection in ad hoc networks*, IEEE Internet Computing, Volume 9 number 6 pages 34-51, December 2005.

[8] Y. Sun, Z. Han, W. Yu, K. J. Ray Liu, *A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks*, In Proceedings of IEEE Infocom'06, 2006.

[9] Q. Ding, X. Li, M. Jiang, X. Zhou, *Reputation-based Trust Model in Vehicular Ad Hoc Networks*, International Conference on Wireless Communications and Signal Processing, Suzhou 2010.

[10] F. Dotzer, L. Fischer, P. Magiera, *VARS: A vehicle Ad hoc network reputation System*, Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, WoWMoM 2005, Taormina-Giardini Naxos 2005.

[11] G. Hachtel, E. Macii, A. Pardo and F. Somenzi, *Markovian Analysis of Large Finite State Machines*, Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on , Volume 15, Number 12, December 1996.

[12] A. Patwardhan, A. Joshi, T. Finin, Y. Yesha, *A Data Intensive Reputation Management Scheme for Vehicular Ad Hoc Networks*, 3^{rd} Annual International Conference on Mobile and Ubiquitous Systems-Workshops, MOBIQUITOUS 2006, July 17-21 San Jose, California, 2006.

[13] A. Rachedi, A. Benslimane, *Toward a cross-layer monitoring process for mobile ad hoc networks*, Security and Communication Networks Volume 2, Issue 4, pages 351 – 368, July/August 2009.

[14] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux *Eviction of Misbehaving and Faulty Nodes in Vehicular Networkss*, IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks ,O ctober 2007.

[15] C. Sommer, R. German and F. Dressler, *Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis* , IEEE Transactions on Mobile Computing, pages 3-15, Vol. 10 No. 1, January 2011.

[16] A. Iyer, A. Kherani, A. Rao, and A. Karnik, *Secure V2V communications: Performance impact of computational overheads*, IEEE INFOCOM 2008 IEEE Conference on Computer Communications Workshops, 2008.