DTM^2: Adapting job market signaling for distributed trust management in vehicular ad hoc networks

Nadia Haddadou, Abderrezak Rachedi

DTM^2: Adapting Job Market Signaling for Distributed Trust Management in Vehicular Ad Hoc Networks

Nadia Haddadou, and Abderrezak Rachedi
Université Paris-Est - Gaspard Monge Computer Science Laboratory (LIGM - UMR 8049)
75420 Champs sur Marne, France

***Abstract*—In this paper, we address the issue of the presence of malicious and selfish nodes in Vehicular Ad Hoc Networks (VANETs). Malicious nodes spread false and forged messages, while selfish nodes only cooperate for their own interest. To deal with this, we propose DTM^2, a Distributed Trust Model inspired by Spence's Job Market model from Economics. In our model, a sender node transmits a signal with its message. This signal represents a guarantee of the truthfulness of the message for the potential receivers. In order to use the signal, the sender node has to pay a cost, which depends on the value of the signal and its own behavior. Therefore, the worse the behavior of the sender node, the more expensive the signal cost. This model deters the sender nodes from acting as malicious nodes. Similarly, cooperation of the sender nodes is rewarded proportionally to the signal's value. We validated DTM^2 via extensive simulation in an urban scenario. We show that our approach is able to detect and evict gradually all malicious nodes in a network composed of 25%, and 50% of them. Moreover, our solution greatly decreases the ratio of corrupted and false data sent through a network to levels as low as 0%, and it increases the participation ratio of selfish nodes by 20%.**

I. Introduction

Vehicular Ad Hoc Networks (VANETs) are collaborative networks having several particular properties, such as high mobility, predefined mobility scenarios, frequent topology changes, and few operational limitations (e.g. memory, processing, energy,...). They offer a wide variety of applications, ranging from driver and passenger comfort applications to road safety applications. In the latter, nodes broadcast their collected data, and relay other's messages in order to inform all participants about traffic conditions, and alerting them in case of accidents [1]. In this work, we are interested in this kind of applications when they are deployed in VANETs without any communication infrastructure, and requiring advanced dissemination algorithms, such as [2] and [3].

Certain safety applications, such as advanced driver assistance systems, are very important, and may cause unsafe situations on road traffic in case of misappropriation. Therefore, a node should never accept any safety information without guarantee on its truthfulness. Moreover, since safety applications are time sensitive, a node has to quickly make a decision about the validity of a received message. This task becomes even more challenging when the VANET infrastructure is scattered or non-existent, because it is impossible to validate any information beforehand.

In this work, we focus on two issues. First, we propose an effective solution that filters out the nodes that introduce false information or retransmit distorted information in a VANET. These nodes are called *malicious* nodes. In a VANET, some of the nodes can be strictly malicious, while others can alter their behavior from good to bad (e.g. sending false information) and vice-versa. Second, we tackle the problem of *selfish* nodes. Selfish nodes act to serve their own interests and use their resources only for their own needs. Thus, their cooperation rate is low. Unlike malicious nodes, these selfish nodes are rational, which means that they can cooperate if it is in their interest.

In a collaborative network such as a VANET, any node dissociation is difficult because of the significant number of nodes composing the network. On top of that, because of high mobility and extended deployment areas, asymmetric information regarding the behavior of each node is widely disseminated. Therefore, establishing direct connections between nodes becomes challenging, thus encouraging the emergence of malicious and selfish nodes. In order to deal with node scattering, we allocate each node a credit account, which can increase and/or decrease according to its behavior. This credit is useful to obtain advantages in the network, such as receiving other nodes' messages. Holding credits allows a node to take part in the network by sending or receiving messages. On the other hand, a node that runs out of credits is evicted from the network.

In order to manage the nodes' credit, we based our solution on an economics model called the Job-Market model [4], belonging to the signaling models [5]. These models intervene in the case of asymmetric information [6], and thus can be used to have a global view of nodes' behavior in VANETs. In addition, the high mobility of vehicles and their large deployment area, cause sporadic connections in the network, and infrequent meeting intervals among nodes [7]. Moreover, since reputation models need stable connections to obtain actual reputation values, and may take a long time to eradicate one misbehaved node, a reputation model for VANET is not enough. The main concept behind signaling models is to exchange signals between nodes. The signal is a characteristic of the node's truthfulness. It has a cost corresponding to the

actual behavior of the node. Thus, this cost is a guarantee of the node's truthfulness. If a sent message is considered as false and thus refused by the neighbors, the emitting node loses its signal cost and incurs an eviction from the network.

To summarize, the contributions of our work are:

- A distributed trust model for VANETs, inspired from the Job Market Signaling model.
- A prevention mechanism, in order to detect and evict malicious nodes from the network.
- An incentive mechanism, to increase the selfish nodes' cooperation.

The remainder of this paper is organized as follows: In Section II we present the related works dealing with trust models in literature. In Section III we present our solution. Section IV presents our performance study and our simulations results. Finally, Section V concludes this paper and presents our future works.

II. Related Work

There are many solutions proposed in literature dealing with trust models for mobile ad-hoc networks as presented in the survey [8]. These solutions cope either with malicious nodes or selfish ones, but rarely with both of them at the same time.

To improve the cooperation in a network, existing solutions propose rewards in return of a node's participation, which is the general concept of incentive cost/reward models, as presented in [9], [10] and [11]. These solutions use nuggets or virtual money as method of payment to incite nodes to be more cooperative.

Buttyàn et al. propose two schemes to estimate a node's reward for a retransmission, the packet purse model and the packet trade model [9]. The first scheme estimates rewards according to the number of intermediate nodes. However, because of the propagation speed of information in VANETs [12] and the high mobility of vehicles, underestimation and overestimation of the reward occur, which leads the solution to be ineffective. In the second scheme, the destination node has to reward all intermediate nodes for their forwarding actions, which represents an expensive cost if there are many of them. Furthermore, both these schemes deal only with selfish nodes.

The second solution [10] proposes different levels of cooperation for network's nodes. These levels can make the participation turn into a quantitative one and not necessarily a constant one, thus leading to declines in the network's connectivity. The third solution is based on the presence of a Credit Clearance Service to verify the receipts of all the actions in the network, and then reward the participants [11]. The use of this method can increase the network delays, and negatively impacts its performance.

Another kind of solutions based on the use of a reputation model for vehicles, is proposed by Minhas et al. [13]. The basic idea is to add a criterion about the category of the driver, setting apart, for instance, a law enforcement agent from a regular citizen. To validate a received message, a node asks its neighbors about its validity, and it takes it into consideration only if the received responses reach a majority consensus. The limitations of this solution concern performance due to the generated overhead, and the time that it can take to validate received data. Another solution uses fairness as criterion for cooperation by computing reputation values, so that nodes cooperate with each other in a reciprocal way [14]. However, this solution involves huge costs caused by the monitoring as demonstrated in [15].

Our solution, DTM^2, is able to cope with the presence of both malicious and selfish nodes in a VANET without any infrastructure. The computation of signaling costs and reward values are not based on estimation, which leads our approach to handle more easily the high mobility of a VANET. DTM^2 creates an auto-selection among the nodes to evict malicious nodes and to increase the cooperation of selfish ones, without impacting the performance of the network.

III. DTM^2: Distributed Trust Model Inspired from Job-Market

DTM^2, is a solution inspired from the Job-Market model proposed by Spence [4], which belongs to the signaling models [5]. These models are used in asymmetric information cases, and bring solutions mainly in the form of equilibriums.

In the economics market of labor, asymmetric information concerns the employees and employers during a hiring. In this case, an employer has no way to ascertain the productive capacity of an employee before hiring him, while an employee is fully aware of it. Spence addresses this problem by transforming the communication between both parts into a signaling game. An employee uses his academic degrees as a signal to an employer, in order to distinguish himself from the other employees, thus influencing the employer to hire him. Spence's model differs from other signaling models because, unlike other models, a signal has no other purpose but to be used for the signaling function.

A signal has a cost. In Spence's model this cost has to be negatively correlated with the production capacity of a signaler. This allows an auto-selection of the members in a group. Each member uses the signal value, which maximizes its benefits; and because signaling costs are cheap for highly productive members, they use a great signal value. Moreover, the model prevents low-productive members from cheating by establishing expensive signaling costs for them, thus disabling them from imitating highly productive members.

A. Problem Formulation

Spence's model is adaptable to a VANET, since nodes in this kind of networks also suffer from asymmetric information regarding the behavior of each one of them. Because of long and infrequent meeting intervals, it is difficult to establish valid and truthful links between nodes only by using a reputation model. Also, this model increases cooperation among nodes, by offering them rewards positively correlated with their behavior. This represents a strong incentive to the selfish nodes. Regarding malicious nodes, they are detected and evicted when they run out of credit, which happens after a number of malicious actions.

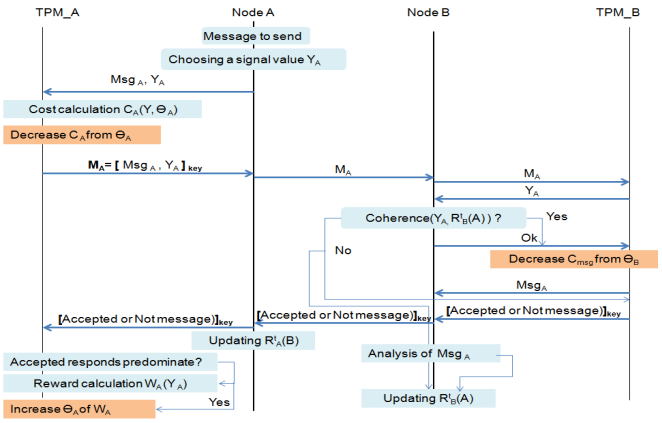

Fig. 1. Message exchange using DTM^2

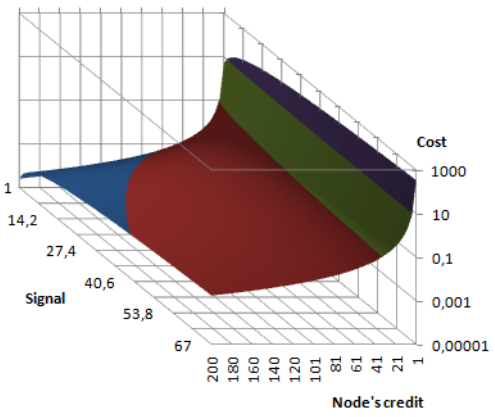

Fig. 2. Signaling cost values for different signal values and nodes' credit

Our solution replaces the academic signal of Spence's model by a value signal, observable by all, and used when sending a message as a guarantee of its truthfulness. The signal cost depends on the remaining credit of each node. Upon their first connection to the network, each node receives the same amount of credit. This credit is used to pay the signaling cost when sending a message, and to decrypt received messages. It increases when a sent message is approved by a majority of recipient nodes.

B. DTM^2 Process

In order to secure this mechanism, we assume that each node has a Trusted Platform Module (TPM) [16]. A TPM is a secure hardware that is able to generate keys, and to encrypt messages. In this way, a node is able to encrypt its sensitive information. The TPM manages the credit count of nodes. It stores the credit in its shielded location, then it computes and deducts the signaling cost, in the case of sent messages; or deducts the price of a received message in case of it is validated by the receiver. It also increases the credit count when a sent message is accepted by the majority of its recipients. Finally, the TPM stores a fingerprint of the application it is responsible for (e.g. an advanced driver assistance system), which leads it to detect any changes to the application made by an attacker.

Fig. 1 illustrates the general functioning of DTM^2. In this example, node A broadcasts a message that is received by node B. First, node A chooses a signaling value Y_A. This value is attached to its message Msg_A, and both of them are sent to its TPM. TPM_A uses the credit count of node A, θ_A, to compute the corresponding cost, C_A, of its signal value Y_A, and then subtracts it from the credit count. To ensure the integrity of the mechanism, the TPM signs the message, M_A, which contains both the signal value Y_A and the data to share, Msg_A, using its private key, and then returns it to node A.

When node A broadcasts message M_A, node B receives it and asks its TPM, TPM_B, to decrypt the signal value for it in order to evaluate its coherence with the reputation value it holds on node A, $R^t_B(A)$. If the reputation is coherent, then node B accepts the message and asks TPM_B to decrypt the rest of the message, which contains the data. Then, its TPM subtracts the cost of receiving a message, C_{msg}, fixed by the application; and delivers the decrypted data, while returning a signed acceptance message about the received information to node B, which will be sent to the source node. In case B refuses the message, a signed refusal message from TPM_B is sent to the source node A.

In both acceptance and refusal cases, the reputation values of both nodes A and B are updated, for the sent message for A, and for the acceptance or refusal message for B, as described in [17]. Finally, if node A receives a majority of positive returns from its recipients, then TPM_A increases its credit count by a reward, W_A, proportional to its used signal value Y_A.

In the following subsections, we detail the signaling cost and reward functions, and the incentive and preventive mechanisms of the trust model with respect to the net benefit of a node.

C. Computation of the Signaling Cost

In highly mobile environments, such as the one under consideration, the signal Y used by a source node acts as a guarantee about the validity of its messages and its honest behavior. An optimal signal value maximizes the net benefit of a node. This occurs when a signal corresponds to the real behavior of the node, which is unavailable to the network and unknown by its TPM. As the credit count value does not change with mobility, this information can be used as a hint on its behavior, since the more a node cooperates well, and the more recipients accept its messages, the more its credit increases thanks to rewards and vice-versa. This information is stored by the node's TPM. The signaling cost, C, is negatively correlated to the credit count, θ, but positively correlated to the signaling value according to the two conditions of the Job-Market model, as shown in (1). The first condition is met when $\frac{\partial C}{\partial Y} > 0$; and the second when $\frac{\partial C}{\partial \theta} < 0$ and $\frac{\partial^2 C}{\partial Y \partial \theta} < 0$.

$$\begin{cases} C(Y_1, \theta) > C(Y_2, \theta) & For \quad Y_1 > Y_2, \\ C(Y, \theta_1) < C(Y, \theta_2) & For \quad \theta_1 > \theta_2, \end{cases} \tag{1}$$

The signaling cost computation is presented in equation (2). It uses two positive real coefficients β and α, in order to

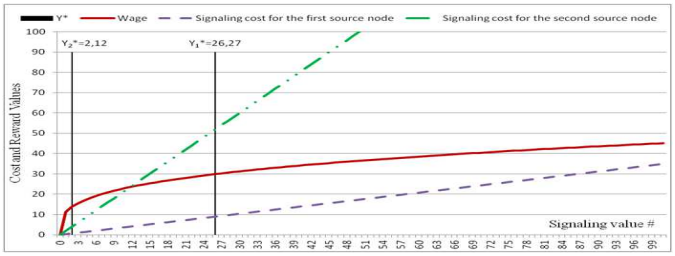

Fig. 3. Cost and reward curves for different signal values

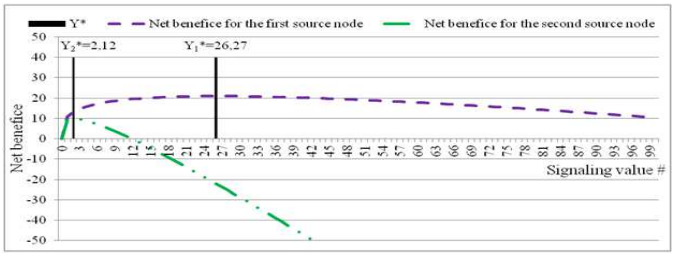

Fig. 4. Net benefit curves for different signal values

normalize the signal value regarding the credit count of a node. The values of β and α are fixed by the VANET application from the start. Fig. 2 illustrates the behavior of the signaling cost for various values of both the signal and node's credit, using β=5 and α=2.3. We can clearly notice that the fluctuations of the node's credit has a larger impact on the cost than the signal value.

$$C(Y,\theta) = \frac{\beta \times Y}{\theta^{\alpha}} \tag{2}$$

where β, α, θ >0

To demonstrate the negative and positive correlations required by the model, the derivatives of the cost function with respect to the signal value, the node's credit, and the second derivative, are given in (3).

$$\begin{cases} \frac{\partial C}{\partial Y} & = \frac{\beta}{\theta^{\alpha}} > 0 \\ \frac{\partial C}{\partial \theta} & = \frac{-\alpha \times \beta \times Y}{\theta^{\alpha+1}} < 0 \\ \frac{\partial^2 C}{\partial Y \partial \theta} & = \frac{-\alpha \times \beta}{\theta^{\alpha+1}} < 0 \end{cases} \tag{3}$$

To avoid cheating or security problems when a node pays a signaling cost, the TPM calculates the cost and deducts it from the node's credit. It then encrypts the message containing both the data to share and the signal value by using its secret key, and returns it to the node.

D. Computation of the Reward Value

To motivate nodes to cooperate, DTM^2 proposes incentive rewards to truthful nodes for their sent messages. A reward value depends on the signal used by the source node. The secondary goal of this reward is to obtain an auto-selection of the nodes, which we name a *separating equilibrium*, by inciting them to maximize their benefit by not cheating on their used signal value. The advantage of an auto-selection is that it copes with frequent changes to the topology, as often found in VANETs.

In this model, a reward W is always greater than the cost paid by a node, provided that the node uses a signal corresponding to its credit. The two conditions given in (4), concern the reward on this model. The first condition concerns the rationality of a node. Each node chooses to use a signal Y to maximize its net benefit. This is found when the derivative of the wage is equal to the derivative of the cost with respect to the signal value. The second condition, sets the initial wage value, which has to be known beforehand by the nodes. Since the credit count of a node hints the real behavior of a node, the initial wage value depends on it to make it proportional to the real behavior of the node. The initial wage is set by dividing the credit of a node by a coefficient σ, such that the more σ is high, the more the application is strict regarding the final wage.

$$\begin{cases} \frac{\partial W}{\partial Y} & = \frac{\partial C}{\partial Y}(Y,\theta) \\ W & = \frac{\theta}{\sigma} \end{cases} \tag{4}$$

where σ>0

The resolution of this system, obtained by integrating Y's value assuming that the minimum value of W and Y is equal to 0, gives us the final equation of the wage shown in (5):

$$\begin{cases} \frac{\partial W}{\partial Y} & = \frac{\beta}{\theta^{\alpha}} \\ \theta & = W \times \sigma \end{cases}$$

$$\begin{aligned} \frac{\partial W}{\partial Y} & = \frac{\beta}{(W \times \sigma)^{\alpha}} \\ W^{\alpha} \times \frac{\partial W}{\partial Y} & = \frac{\beta}{\sigma^{\alpha}} \\ \int_0^{\infty} W^{\alpha} \times \frac{\partial W}{\partial Y}\ \partial Y & = \int_0^{\infty} \frac{\beta}{\sigma^{\alpha}}\ \partial Y \\ \frac{[W^{\alpha+1}]}{\alpha+1} & = \frac{\beta}{\sigma^{\alpha}} \times [Y] \\ \frac{W^{\alpha+1}}{\alpha+1} & = \frac{\beta \times Y}{\sigma^{\alpha}} \end{aligned}$$

$$W = [\frac{\beta \times (\alpha+1) \times Y}{\sigma^{\alpha}}]^{\frac{1}{\alpha+1}} \tag{5}$$

The reward value is added to the credit count of a source node by its TPM, providing that its sent message is validated by the most of the recipients. To verify this, each recipient notifies its own TPM about its decision regarding a received message, and an encrypted message about its decision of acceptance or not is sent to the source node. The message is encrypted to avoid case where a node accepts the received information but sends the refusal message to sabotage the source.

E. Optimum Signal Value

This model is designed in such a way that a node makes the maximum benefit when it uses the optimum signal value $Y^{\star}$ regarding its credit. The optimum signal for each node is obtained from equation (5), by replacing W by $\frac{\theta}{\sigma}$. The result is given in equation (6).

$$Y^{\star} = \frac{\theta^{\alpha+1}}{\sigma \times \beta \times (\alpha+1)} \tag{6}$$

Failure to respect $Y^{\star}$ causes a shortfall or a loss in credit, as illustrated in Fig. 3. This figure depicts two curves representing the signaling cost of two nodes, and another curve showing the received wage when the sent message is accepted. The

TABLE I
SIMULATION PARAMETERS

Number of nodes:100	Mac layers protocols: IEEE 802.11
Transmission range: 250 m	Simulation time: 3600s
Bandwidth: 11 Mbps	Area size: $3 \times 3\ Km^2$
Diffusion data algorithm: ADCD [2]	
C_{msg}=$C(Y^\star, \theta_{initial})/5$	Speed: 30-50 km/h
β=$3.5 \cdot 10^4$	α=2.3
σ=5	$\theta_{initial}$=100

first source node possesses 150 credits (i.e it has had a good behavior), and the second source node possesses only 40 (i.e it has had a bad behavior), given that the initial credit of the application $\theta_{initial}$ is 100 credits. These curves show results for different signaling values ranging from 0 to 100, and are obtained by setting $\beta = 3.5 \cdot 10^4$, α=2.3, and σ=5 . We notice that the wage of the first node is more advantageous. But a shortfall is present for the two when they do not use the optimal signal values, which are $Y_1^\star$ and $Y_2^\star$, respectively.

The net benefit NB of the two nodes is observable in Fig. 3. It is at its maximum when the signaling value equals $Y^\star$. Its equation is given in (7) and the results using the same parameter values as before are illustrated in Fig. 4.

$$\begin{aligned} NB &= W - C \\ NB &= [\tfrac{\beta \times (\alpha+1) \times Y}{\sigma^\alpha}]^{\frac{1}{\alpha+1}} - \tfrac{\beta \times Y}{\theta^\alpha} \end{aligned} \tag{7}$$

Fig. 4 presents the curves of the net benefit for the two source nodes. We notice that the curve of the second node, which is less truthful than the first, decreases faster when it does not respect its optimum signal $Y^\star$. This clearly shows that because of bad behavior, nodes quickly exhaust their credit and are therefore evicted from the network.

F. Received Message Acceptance Process

A second way to encourage nodes to cooperate is to create the need for holding credits and earning them. For this reason, decrypting a received message is paid in this model. In the case where a node is selfish, its credit decreases slowly because of its inexistent or insufficient cooperation. To secure this part of the model, the cost of a received message, C_{msg}, is fixed by the application, and subtracted from a recipient node's count by its TPM. This is only done in case of acceptance by the recipient. A validation decision is made with respect to the following two criteria:

- The reputation of the source node, held by the receiver.
- The used signal value by the source node.

The used reputation, $R_r^t(s)$, belongs to [0, 1], and is calculated at time t by the Receiver node r with respect to the source node, s. This reputation is local and is not shared in the network. Therefore, it is a firsthand reputation. If it is too bad, it represents an elimination criterion for the received message. This criterion is very important at the start of the application, when all the nodes have the same amount of credits and thus use the same signaling value. Its calculation can be done as described in [17].

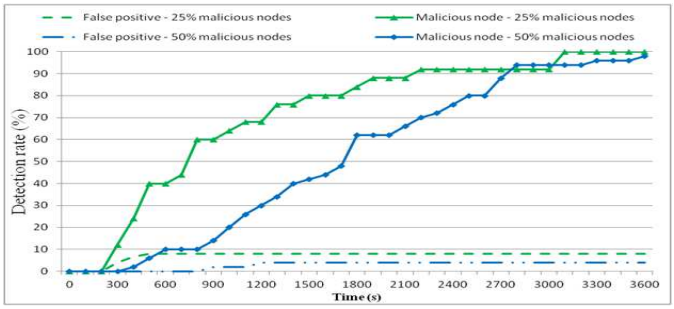

Fig. 5. Percentage of detected nodes: malicious and false positives

After verifying the reputation criterion, a recipient node can base its acceptance on the signal used by the source. A minimum accepted signal is generally fixed to the value of the optimal signal value, $Y^\star$, for a node detaining only 20% of $\theta_{initial}$.

IV. PERFORMANCE EVALUATION

A. Simulation Setup

We evaluate the performance of our model by focusing on its ability to detect and evict malicious nodes, and to incite selfish nodes to cooperate more. In our scenario, a malicious node is a node that creates and sends false information, and that corrupts data before sending it during a retransmission. On the other hand, selfish nodes only participate out of self-interest (i.e. when they do not have enough credit to decrypt received messages). To this end, we first measure the detection rate and average ratio of corrupted data respectively, in a network composed of 25% and 50% of malicious nodes. Then, the average data reception ratio is measured in a network composed of 25% and 50% of selfish nodes.

We conduct a set of simulations on $NS2$ [18] using VanetMobisim [19] as vehicular mobility model in an urban scenario. We compare DTM^2 with a network not using any solution, and a network using a majority-based and experience-based trust model presented in [13], which we refer to as MEB_Trust. The basic idea in MEB_Trust is that a node asks its neighbors, according to their categories, about the truthfulness of a received data, and considers it only if it reaches a majority consensus. This solution depends on the presence of trusted entities (e.g. police cars), which always respond correctly to nodes. For our simulation of this solution we include 3 police cars. The other simulation parameters are shown in Table I.

B. Result Analysis

The percentage of detected nodes for different compositions of malicious nodes in the network is illustrated in Fig. 5. A node is detected and evicted when it runs out of credits. The results show that the percentage of detection gradually increases, relatively quickly according to the number of malicious nodes in the network. Our solution is able to detect 50% of malicious nodes at around $800s$, and it reaches 100% at around $3100s$ in a network composed of 25% of malicious nodes. Moreover,

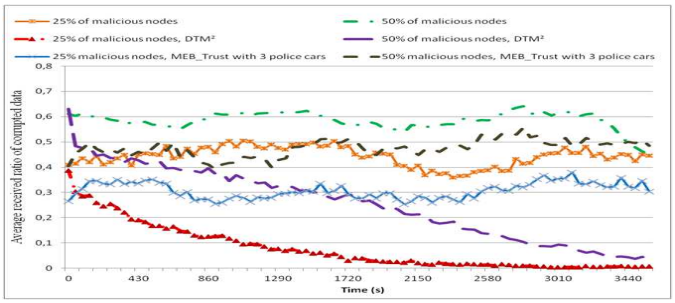

Fig. 6. Average received ratio of corrupted data with 25% and 50% of malicious nodes

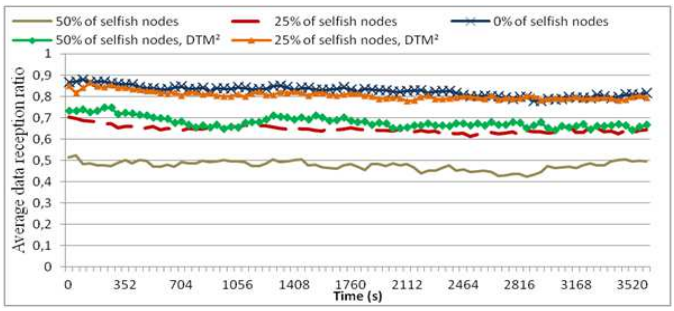

Fig. 7. Average ratio of received data with 0%, 25% and 50% of selfish node

the false positive percentage does not exceed 8%, which means that a good behavior node is rarely mistakenly detected as being malicious.

Fig. 6 presents the average ratio of received corrupted data from malicious nodes, or retransmitted by good behavior nodes by mistake, in a network composed of 25% and 50% of malicious nodes. We note that when using DTM^2, this ratio quickly decreases until reaching 0 after $2500s$ of simulated time for a network composed of 25%, and achieves a ratio of around 0.05 after $3600s$ of simulated time in a network composed of 50%. Moreover, while all malicious nodes have been evicted from the network when their credit is exhausted by using DTM^2, it is not the when using MEB_Trust.

The effectiveness of our solution regarding its ability to incite selfish nodes to cooperate is visible on Fig. 7. The benefits of using our solution becomes evident, as the average data reception ratio in the presence of 25% of selfish nodes is the same that for the ideal case when no selfish nodes are present. This is because the need of obtaining credits is created among selfish nodes, since they need credits to decrypt their received messages. Moreover, when in the presence of 50% of selfish nodes, the average data reception ratio using DTM^2 is greater than the case where there is no deployed solution ratio in the presence of 25% of them.

V. Conclusion

In this paper, we proposed DTM^2, a Distributed Trust Model for VANETs, adapted from Job Market Signaling, a well-known economics model used in case of asymmetric information. DTM^2 focuses on managing a tamper-proof credit count received by nodes at the start of the application. In order to detect and evict malicious nodes, it creates an auto-selection among the network's nodes and exhausts the credit for those nodes with bad behavior. Moreover, to improve the cooperation level of selfish nodes, it proposes inciting rewards. We showed via simulation the achievement of these two objectives in networks composed of 25%, and 50% of malicious or selfish nodes. In both of these cases, DTM^2 is able to gradually detect *all* malicious nodes and completely eliminate their negative effects on the network, while maintaining a low percentage of false positives. Furthermore, our approach is able to increase the cooperation of selfish nodes by 20% with respect to networks where no solution is deployed.

As future work, we aim to improve our model to be used in different high mobility scenarios, and in combination with more sophisticated attacker models.

References

[1] D. Camara, C. Bonnet, and F. Filali, "Propagation of public safety warning messages: a delay tolerant network approach," in *IEEE WCNC*, Sydney, Australia, April 2010.

[2] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "Modeling and performance evaluation of advanced diffusion with classified data in vehicular sensor networks," *Wireless Communications and Mobile Computing*, vol. 11, no. 12, pp. 1689–1701, Oct. 2011.

[3] C. Wu, S. Ohzahata, and T. Kato, "A broadcast path diversity mechanism for delay sensitive vanet safety applications," in *IEEE VNC*, Amsterdam, The Netherlands, 2011.

[4] M.Spence, "Job market signaling," *The Quarterly Journal of Economics*, vol. 87, no. 3, pp. 355–374, 1973.

[5] J. Sobel, "Signaling games," *Computational Complexity Theory, Techniques, and Applications*, pp. 2830–2844, 2012.

[6] M.Spence, "Signaling in retrospect and the informational structure of markets," *The American Economic Review*, vol. 92, no. 3, pp. 434–459, 2002.

[7] E. Baccelli, P. Jacquet, B. Mans, , and G. Rodolakis, "Information propagation speed in bidirectional vehicular delay tolerant networks," in *IEEE INFOCOM*, Shanghai, China, April 2011.

[8] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile ad hoc networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. Preprint, pp. 1–20, 2011.

[9] L. Buttyán and J. Hubaux, "Enforcing service availability in mobile ad-hoc wans," in *ACM MobiHoc*, Boston, USA, Aug 2000.

[10] ——, "Stimulating cooperation in self-organizing mobile ad hoc networks," *ACM/Kluwer MONET*, vol. 8, pp. 579–592, 2001.

[11] S. Zhong, J. Chen, and Y. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *IEEE INFOCOM*, San Francisco, USA, Apr. 2003.

[12] Z. Zhang, G. Mao, and B. D. O. Anderson, "On the information propagation process in multi-lane vehicular ad-hoc networks," in *IEEE ICC*, Ottawa, Canada, June 2012.

[13] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expended trust management for agents in vehicular ad-hoc networks," *International Journal of Computational Intelligence: Theory and Practice(IJCITP)*, vol. 5, no. 1, pp. 03–15, Jun. 2010.

[14] M. Ashtiani and Q. Dongyu, "Achieving fair cooperation for multi-hop ad hoc networks," in *QBSC*, Queen's University Kingston, Canada, May 2010.

[15] A. Rachedi and A. Benslimane, "Toward a cross-layer monitoring process for mobile ad hoc networks," *Security and Communication Networks, John Wiley InterScience*, vol. 2, no. 4, pp. 351–368, 2009.

[16] "Trusted computing group: Tpm main specification. main specification version 1.2 rev. 116," March 2011.

[17] Z. Charikleia, L. Brian, H. Marek, and K. Roshan, "Robust cooperative trust establishment for manets," in *ACM SASN*, New York, USA, 2006.

[18] The NS-2 website. [Online]. Available: http://www.isi.edu/nsnam/ns/

[19] M. Fiore, J. Härri, F. Fethi, and C. Bonnet, "Vehicular mobility simulation for vanets," in *IEEE ANSS*, Norfolk, USA, Mar. 2007.