A Multidimensional Trust Model for Vehicular Ad-Hoc Networks

Maryam Najafi, Lyes Khoukhi, Marc Lemercier

A Multidimensional Trust Model for Vehicular Ad-Hoc Networks

Maryam Najafi[1], Lyes Khoukhi[2], Marc Lemercier[1]
[1]*Computer science and digital society (LIST3N) Laboratory, University of Technology of Troyes (UTT), Troyes, France*
[2]*Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France*

maryam.najafi@utt.fr, lyes.khoukhi@ensicaen.fr, marc.lemercier@utt.fr

***Abstract*—In this paper, we propose a multidimensional trust model for vehicular networks. Our model evaluates the trustworthiness of each vehicle using two main modes: 1) Direct Trust Computation DTC related to a direct connection between source and target nodes, 2) Indirect Trust Computation ITC related to indirectly communication between source and target nodes. The principal characteristics of this model are flexibility and high fault tolerance, thanks to an automatic trust scores assessment. In our extensive simulations, we use Total Cost Rate to affirm the performance of the proposed trust model.**

Keywords—VANET, Malicious Nodes, Security, Trust, Vehicular Ad-Hoc Network

INTRODUCTION

Vehicular communication technology provides two types of communications: 1) Vehicle to Vehicle (V2V) to offer a secure network and safe exchange of information between nodes (i.e., vehicles), and 2) Vehicle to Infrastructure (V2I) in which vehicles exchange messages with road infrastructures [1, 2]. As illustrated in Fig. 1, the main two components of the vehicular network are On-Board Units (OBUs) and Road Side Units (RSUs) [3], which are deployed along the road. The main purpose of vehicular technology is to prevent accidents, improve traffic control systems and enable safer driving [4]. However, the vehicular network is prone to critical risks, threats, and attacks due to its unique characteristics and dynamic topology.

Several trust models have recently been suggested to improve the security in vehicular networks. However, most of them do not consider a variety of behavioral conditions and uncertain situations. There are two types of trust models: centralized trust management mechanisms and decentralized trust management mechanisms. The most crucial difference between these two mechanisms is "determining the responsibility for providing trust data". In a centralized mechanism, the nodes request trusted data from a centralized trust manager, but the nodes are responsible for providing the trusted data in a decentralized mechanism. These strategies are based on pseudonyms, reputation systems, clustering (i.e., header cluster and member cluster), blockchain, etc. However, under different conditions, there are no ways to compare how they would behave effectively in practice. Each of these models has advantages and disadvantages [5 - 9]. We decided to take the benefits of each to design our model.

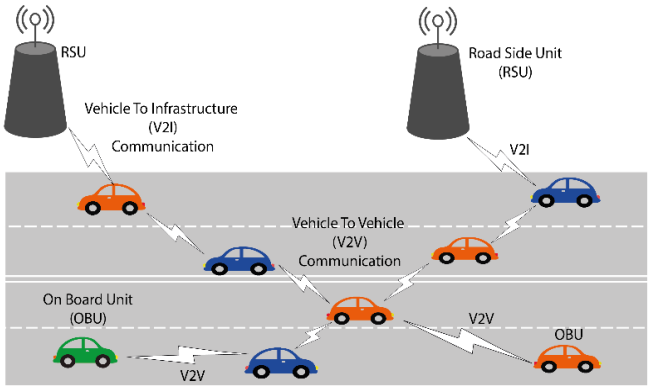


Fig. 1. The global architecture of Vehicular Ad-Hoc Network

To improve trust in the vehicular networks, we propose a robust multidimensional trust model that evaluates trust using two main modes. 1) Direct Trust Computation (DTC) in this part, we use the advantages of the decentralized model. In DTC, the source node has a direct connection with the target node so that the source node can evaluate the trust of the target node by the watchdog technique and Bayes' theorem [10]. The score that is obtained from direct connection has more impact than indirect connection. 2) Indirect Trust Computation (ITC) in this part, we use the advantage of the centralized trust model. ITC can observe the behavior of the target node with its neighbors by RSUs. In other words, the source node will use the recommendations of the neighbors' target node, which receive direct connection from the neighbors' target node with the target node

The final trust score is a combination of DTC and ITC trust computations modes. We carried out extensive simulations to demonstrate the performance of our model by calculating the Total Cost Rate, which is based on both accuracy and error parameters.

The rest of the paper is organized as follows. The proposed multidimensional trust model is explained in next section. We will describe the validity and simulation of the proposed model and finally our conclusion in the last section.

A MULTIDIMENSIONAL TRUST MODEL

The main focus of this paper is to present a secure model to evaluate the trust of each node and mitigate malicious behavior of vehicular nodes. We propose a robust multidimensional trust model that evaluates the node's trust score. Our model considers three types of messages usually employed in vehicular environments: 1) periodic messages; 2) urgent event messages, and 3) traffic messages. To calculate the vehicle's trust, we use the Bayesian filter and the watchdog technique to measure the trust scores of vehicles accurately. The architecture of our proposed model is illustrated in Fig. 2. This trust score is a combination of Direct DTC and Indirect ITC trust computation modes.

A. Direct Trust Computation

To evaluate a node's trust based on a DTC mode, the source node must be connected directly to the target node so that the source node can assess the target node's trust. The score that is obtained from the direct trust is called Primary score (Ps). To evaluate Ps, we use the watchdog technique and Bayes' theorem. Ps is calculated as follow:

$$Ps\ (i.j) = \beta\ Ps_t(i.j) + (1-\beta)\ Ps_{t-1}(i.j) \qquad (1)$$

We denote the Primary score of node 'i' on node 'j'by $Ps\ (i.j)$ and $Ps\ (i,j) \in [0,1]$. Also, $Ps_{t-1}(i.j)$ represents the last primary score and $Ps_t(i.j)$ represents the current primary score of node 'i' on node 'j'. In this equation, we use β to give more importance to the current primary score than the previous primary score. Although in some cases, the previous Primary score may not be available, so we have set β to address this issue as follows:

$$\beta = \begin{cases} 0.70, & if\ a\ value\ exists\ for\ Ps_{t-1}(i.j) \\ 1, & otherwise \end{cases} \qquad (2)$$

B. Indirect Trust Computation

To evaluate a node's trust based on ITC mode, we need recommendations from adjacent nodes. We consider that the source node has no direct connection with the target node. Therefore, the source node is not able to observe the behavior of the target node with its neighbors. In this case, we use RSUs. In other words, the source node will use recommendations of neighbors' target node, which it obtains from direct connection between neighbors' target node with the target node.

We use RSUs to calculate indirect trust scores, where RSUs store all scores that are based on direct connections between vehicles (Direct trust). When a source node i needs recommendations about target node j, node i demands the recommendations $R(j)$ from a RSU, in other words, all Primary scores of node j.

$$R(j) = Ps(l,j) \mid l = \{1,2,\dots,n\} \qquad (3)$$

$$R(j) \in\ PR\ (l,j), NR\ (l,j) \mid l = \{1,2,\dots,n\}$$

This score obtained from Indirect Trust Computation, called Secondary score $Ss(i.j)$ of node 'i' on node 'j' and $Ss\ (i,j) \in [0,1]$. $Ss(i.j)$ is calculated as follows:

$$Ss(i.j)\ = \sum_{l=1}^{n} \frac{PR\ (l,j)}{PR\ (l,j)+NR\ (l,j)} \qquad (4)$$

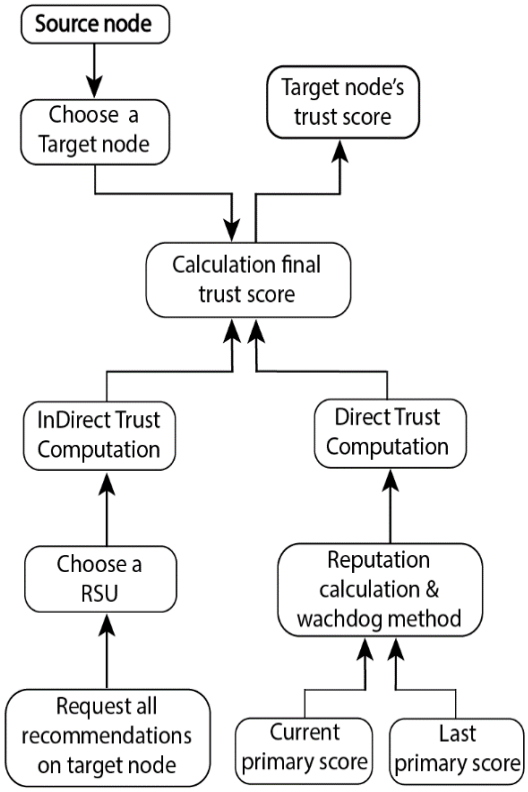


Fig 2. The architecture of our Trust Model

Where $PR\ (l,j)$ is the positive recommendation of node l on node j and $NR\ (l,j)$ is the negative recommendation of node l on node j.

C. Evaluation of Final Trust Score

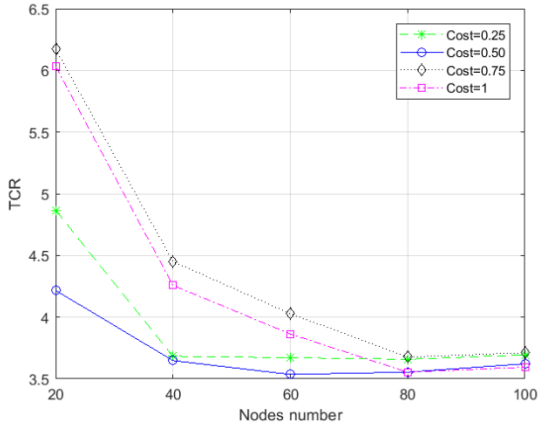
In our model, $FTs\ (i,j)$ denotes the Final Trust score between node 'i' and node 'j'. This score is a combination of the Primary score and Secondary score. However, the Primary score has more impact than the Secondary score on Final Trust Score. The calculation expression of the Final Trust score is:

$$FTs\ (i,j) = \alpha\ Ss(i,j) + (1-\alpha)\ Ps(i,j) \qquad (5)$$

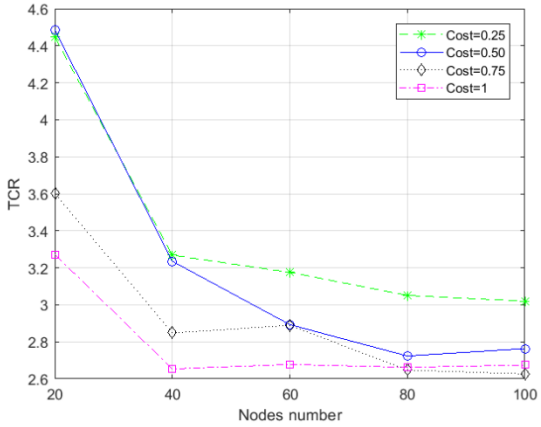
To calculate FTs, we need both the Primary and Secondary scores. However, in some cases, the Primary score may not be available because direct contact is not always possible between the source node and the target node. In addition, the Secondary score is not always available because the target node may not have a neighbor. To tackle these issues, we use α to give weight to the Secondary score and Primary score. We have set α as follows:

$$\alpha = \begin{cases} 0.4, & if\ Ps > 0\ and\ Ss > 0 \\ 1, & if\ Ps = 0\ and\ Ss > 0 \\ 0, & otherwise \end{cases} \qquad (6)$$

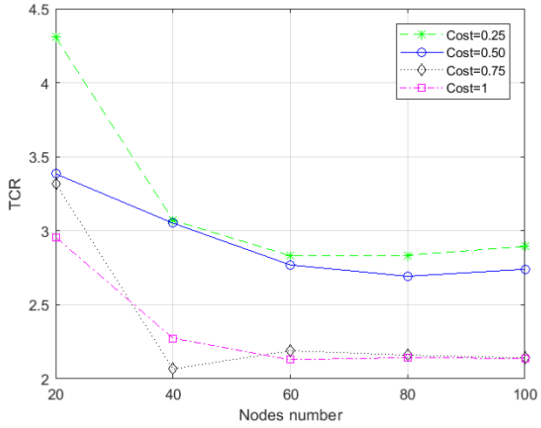
We will assign a state to each vehicle in the vehicular network based on $FTs\ (i,j)$. The value of the Final Trust score is always between zero and one. We defined four possible states for each vehicle (i.e. Malicious (MA), Heavily Suspicious (HS), Lightly Suspicious (LS), and Normal (NO)) as follows:



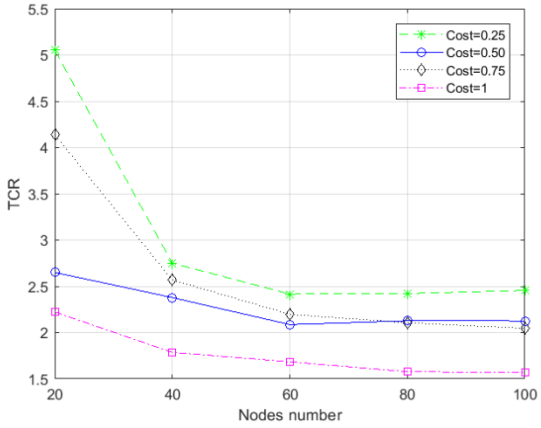
(a) MA: 5%, HS: 5%, LS: 5%, NO: 85%



(b) MA: 10%, HS: 5%, LS: 5%, NO: 80%



(c) MA: 15%, HS: 5%, LS: 5%, NO: 75%



(d) MA: 20%, HS: 5%, LS: 5%, NO: 70%

Fig. 3. TCR vs. nodes scalability

$$\text{State} = \begin{cases} MA & if\ FVs_{id} > 0.7 \\ HS & if\ 0.5 < FVs_{id} \leq 0.7 \\ LS & if\ 0.3 \leq FVs_{id} \leq 0.5 \\ NO & if\ FVs_{id} < 0.3 \end{cases} \quad (7)$$

VALIDATION

To evaluate the performance of our proposed model, we decided to use Total Cost Rate (TCR), in terms of accuracy and error rate. We must compare these factors with a baseline approach. These two parameters, 1) Accuracy (Ac) and 2) Error (Er), are respectively defined as:

$$Ac = \frac{\sum_{i \in s} n_{i \to i}}{N_{MA}+N_{HS}+N_{LS}+N_{NO}} \quad (8)$$

$$Er = 1 - Ac \quad (9)$$

Where:

- $i, j \in s$, $s = \{MA, HS, LS, NO\}$
- $n_{i \to j}$ denotes the number of nodes in the state i which change their states to state j.
- N_i denotes the total number of nodes in the state i.

The two parameters introduced above do not take into consideration the concept of classification cost. In our model, we consider classification cost, which is denoted C. For each incorrect classification, below, we introduce different values of C depending on the situation.

1. C= 0: A node stays in the same state (e.g., $NO \to NO, LS \to$ LS).
2. C= 1: The transition to one-hop range (e.g., $NO \to LS, LS \to HS$).
3. C= C: The transition to two-hop ranges (e.g., $NO \to HS, MA \to LS$).
4. C= 2C: The transition to three-hop ranges (e.g., $NO \to MA$, $MA \to NO$), is 2C times more costly than 1.

This leads us to define C_Ac and C_Er as follow:

$$\text{C\_}Ac = 1 - \text{C\_}Er \quad (10)$$

$$\text{C\_}Er = \frac{\mu}{2CN_{MA}+CN_{HS}+N_{LS}+N_{NO}} \quad (11)$$

Where:

- μ is equal to $2C * (n_{NO \to MA} + n_{MA \to NO}) + C(n_{NO \to HS} + n_{LS \to MA} + n_{HS \to NO} + n_{MA \to LS}) + n_{NO \to LS} + n_{LS \to NO} + n_{LS \to HS} + n_{MA \to HS} + n_{HS \to MA} + n_{HS \to LS}$.

In order to calculate the model's performance, we have to consider all nodes as honest, and define $\mathrm{C\_}Er^{\#}$ as follows:

$$\mathrm{C\_}Er^{\#} = \frac{N_{MA}}{2CN_{MA}+CN_{HS}+N_{LS}+N_{NO}} \quad (12)$$

Also, the calculation of expression TCR is:

$$TCR = \frac{\mathrm{C\_}Er}{\mathrm{C\_}Er^{\#}} = \frac{\mu}{N_{MA}} > 1 \Leftrightarrow \mathrm{C\_}Er^{\#} < \mathrm{C\_}Er \quad (13)$$

From this equation, we conclude that the value of TCR reflects the model's performance. If TCR is greater than 1, it means the performance is considered acceptable. However, if the TCR value is less than 1, it is better not to use the model, because the error in the model with filtering $\mathrm{C\_}Er$ is more than the baseline $\mathrm{C\_}Er^{\#}$. Therefore, the classification error by the filter $\mathrm{C\_}Er$ must be smaller than the error caused without filter $\mathrm{C\_}Er^{\#}$.

In our simulation, we consider a network with different configurations. Our network was composed of 20, 40, 60, 80, and 100 vehicles, and we considered four classifications of cost 'C' (0.25, 0.50, 0.75, and 1). Then, for each scenario, we varied the proportion of malicious nodes (0.05%, 0.10%, 0.15%, and 0.20%). The purpose of this simulation was to find the best TCR and best configuration for our model in different situations. The result of our extensive simulation is shown in Fig. 3.

In the first scenario, considering 5% malicious nodes, we can observe in Fig. 3 (a) the value of TCR is more than 3.5 (A higher TCR value implies better performance). However, with the increasing of the nodes number, the value of TCR decreases, but it is always greater than 1. When the number of vehicles exceeds 80, TCR values are similar and constant. The best value in this case, is achieved by cost = 0.75. In Fig. 3 (b), we show the result of the second scenario with 10% of malicious nodes. In this case, the value of TCR is between 2.6 and 4.5, which illustrates the performance of our model. When the node numbers increase to 80, the TCR values are stable at all four cost levels. The best cost in the case with 10 percent of malicious nodes in the network is 0.25 and 0.50. For the third scenario Fig 3 (c), where we consider 15% malicious nodes, we can observe that the value of TCR is between 2 and 4.5. In our simulation, when the vehicle number reaches 60, the value of TCR decreases. However, it is always greater than 1. The cost equal to 0.25 always has the best TCR value in different node numbers, as illustrated in fig. 3 (c). In the last scenario Fig. 3 (d) we increase the percentage of malicious nodes to 20 percent of the total nodes. We can observe that the curve with asterisk markers is substantially higher than the rest, which means cost = 0.25 is significant. In addition, the stability of TCR values is very important in our model. When the number of vehicles is between 60 and 100, the curves with diamond markers and circle markers show values between 2.04 and 2.19.

In summary, we consider various configurations for our simulation. We obtained suitable values for TCR, even when the percentage of malicious nodes and nodes numbers increased. These results confirm that our model is accurate and offers great precision. The worst value of TCR is 1.57, although it is acceptable because we demonstrated in equation (13) that if TCR value is more than one, it means our model is accurate and its use is appropriate.

CONCLUSION

Vehicular networks are one of the most fascinating wireless technologies and has attracted a great deal of attention. However, this technology is prone to attacks and threats due to its unique characteristics. In this paper, we presented a multidimensional trust model to make the security in the vehicular networks more robust. This model evaluates the trust of vehicles. To calculate the trust score, we consider two modes of computation: 1) a DTC computation mode based on Bayes theorem and the watchdog method; 2) an ITC computation mode in which RSUs are solicited. Extensive simulations using various network configurations have shown that our trust model is accurate and precise. As future work, we plan to design a punishment scheme in order to isolate rogue vehicles in vehicular environments.

ACKNOWLEDGMENT

The authors would like to thank FEDER, Region GRAND-EST, and the MSER for the financial support of this research.

REFERENCES

[1] H. Peng and X. Shen, "Deep Reinforcement Learning Based Resource Management for Multi-Access Edge Computing in Vehicular Networks," in IEEE TNSE, vol. 7, no. 4, pp. 2416-2428, 1 Oct.-Dec. 2020.

[2] Y. Zhang, L. Zhang, D. Ni, K. -K. R. Choo and B. Kang, "Secure, Robust and Flexible Cooperative Downloading Scheme for Highway VANETs," in IEEE Access, vol. 9, pp. 5199-5211, 2021.

[3] J. Shen, T. Zhou, J. Lai, P. Li, and S. Moh, "Secure and Efficient Data Sharing in Dynamic Vehicular Networks," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8208-8217, Sept. 2020.

[4] H. Khelifi, S. Luo, B. Nour, H. Moungla, Y. Faheem, R. Hussain, and A. Ksentini, "Named Data Networking in Vehicular Ad Hoc Networks: State-of-the-Art and Challenges," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 320-351, Firstquarter 2020.

[5] F. Li, Z. Guo, C. Zhang, W. Li and Y. Wang, "ATM: An Active-Detection Trust Mechanism for VANETs Based on Blockchain," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4011-4021, May 2021.

[6] P. Asuquo, H. Cruickshank, C. P. A. Ogah, A. Lei and Z. Sun, "A Distributed Trust Management Scheme for Data Forwarding in Satellite DTN Emergency Communications," in IEEE Journal on Selected Areas in Communications, vol. 36, no. 2, pp. 246-256, Feb. 2018.

[7] M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi, D. Gaiti, "A Stochastic Approach for Packet Dropping Attacks Detection in Mobile Ad hoc Networks," Computer Networks (ComNET), Elsevier, vol. 121, n°5, pp. 53-64, 2017.

[8] A. Nabet, R. Khatoun, L. Khoukhi, J. Dromard and D. Gaïti, "Towards secure route discovery protocol in MANET," IEEE Global Information Infrastructure Symposium (GIIS 2011), Da Nang - Vietnam. 8 p. 4-6 August 2011.

[9] M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi, D. Gaiti, C. Xiuzhen, "Denial of Service (DoS) Attacks Detection in MANETs Using Bayesian Classifiers," the 21st IEEE Symposium on Communications and Vehicular Technology (IEEE SCVT), Delft, Nov., 2014.

[10] M. Najafi, L. Khoukhi, and M. Lemercier, "Decentralized Reputation Model based on Bayes' Theorem in Vehicular Networks," in Proc., *IEEE Int. Conf. on Commun. (ICC)*, (online), June 2021.