Towards a Self-adaptive Trust Management Model for VANETs

Ilhem Souissi[1], Nadia Ben Azzouna[1] and Tahar Berradia[2]
[1]*Strategies for Modelling and ARtificial inTelligence research Laboratory (SMART Lab), Institut Superieur de Gestion de Tunis, Universite de Tunis, Le Bardo, Tunis, Tunisia*
[2]*Institut de Recherche en Systmes Electroniques Embarques (IRSEEM Lab),ESIGELEC, Rouen, France*

Keywords: Self-adaptive, Trust Management, Decision-making, VANET.

Abstract: The vehicular ad hoc networks (VANETs) aim basically to enhance the traffic safety performance, improve the traffic efficiency and achieve a comfortable driving experience. To reach these purposes, it is crucial to ensure the security of this network. Trust is one of the key challenges for VANET security enhancement. Trust management aims to investigate the relationship between the different entities in the network in order to ensure that only trustworthy messages are delivered to drivers. Solutions for trust evaluation are not self-adaptively adjusted to discriminate between the requirements of each class of applications. Moreover, most of these solutions stand on the reputation to determine the trustworthiness of vehicles. However, reputation is not well-suited in VANET due to the absence of social connections between fast moving and distributed entities. In this paper, we present a self-adaptive trust management model that copes with the specifications of each class of applications in a different way in order to enhance the decision-making process, minimize both time and energy consumption for decision-making and improve the network's security. In addition to reputation, similarity and behavior assessment, our model uses the correlation between the event and contextual information and further the risk assessment for decision-making.

1 INTRODUCTION

Vehicular ad hoc network (VANET) is a distributed and highly dynamic network that mainly includes fast moving entities (vehicles) and Road Side Units (RSUs) (Campolo et al., 2015). VANET supports both Vehicle-to-Vehicle communications (V2V) and Vehicle-to-Infrastructure communications (V2I) in order to exchange real time traffic information. It presents a variety of applications that can be categorized into three main classes: (1) Safety applications that aim to enhance the traffic safety, (2) Traffic management applications that aim to improve the traffic efficiency and (3) Comfort applications that intend to achieve a comfortable driving experience.

However, VANET is vulnerable to many security threats that can disturb the decision-making process (La Vinh and Cavalli, 2014). Therefore, the security of the exchanged messages is critical. Obviously, cryptography is the best-known technique to guarantee the authenticity, the privacy protection and the confidentiality. Nonetheless, the cryptographic materials cannot cope with some issues such as authenticated selfish vehicles, high dynamicity of the network topology, sensor failures, etc. Recently, many researches have been interested in the trust management in VANETs to (1) support the cooperation between entities, (2) detect the selfish and misbehaving ones, (3) ensure a reliable data delivery and (4) enhance the decision-making process.

The existing trust models handle with all of the provided applications by the same way. However, we notice that some of these applications are time-critical and they require high security level such as accident warning applications while the others are not restrictive at all such as restaurant finder applications. Besides, these models rely basically on the reputation, the similarity and the utility assessment (Wei et al., 2014) (Yang, 2013) (Yao et al., 2017). Each kind of these methodologies presents some limitations. First, reputation is not well-suited due to the absence of social connections between fast moving entities. Second, similarity incorporates very simple attributes such as time, location and speed. Only these attributes are not enough to enable a vehicle to find similarities with the other encountering vehicles. Finally, the utility stands on simple and predefined values that cannot ensure an accurate trust evaluation.

Unlike the existing solutions we present a self-adaptive trust model that copes with the requirements

Souissi, I., Azzouna, N. and Berradia, T.
Towards a Self-adaptive Trust Management Model for VANETs.
DOI: 10.5220/0006463305130518
In *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT*, pages 513-518
ISBN: 978-989-758-259-2

of each class of applications in a different way. Accordingly, the contribution of this paper is to enhance the decision-making process that may differ from one situation to another according to the available information. We show that this model can identify multiple kinds of threats such as selfish, dishonest and misbehaving vehicles. It may minimize the required time for trust evaluation and reduce the energy consumption. This model incorporates many concepts such as reputation assessment, similarity between messages and between the recent and the previous sensed events, behavior assessment, correlation between the event and the contextual information and further the risk assessment.

The paper is structured in the following way. In section 2, we present a brief description of the existent trust models as well as the adopted methodologies and their limits. In section 3, the scheme overview is presented. We show the benefit of the proposed self-adaptive trust model through a real life case in section 4. Finally, in section 5, we conclude the paper and we present future directions.

2 RELATED WORK

Trust management has undergone a spectacular evolution in vehicular ad hoc networks for many years to enhance the security and the robustness of such network. Many methods for trust assessment have been proposed in the literature (Zhang, 2011) (Soleymani et al., 2015) (Dwivedi and Dubey, 2016). These solutions depend on prominent methodologies such as reputation, similarity, behavior, etc.

Regarding the reputation-based trust models, the researchers have been focused on the vehicle's trustworthiness to assess the progress of its trust value over the time based on past experiences, direct interactions and recommendations. In (Wei et al., 2014), a trust based framework has been proposed to cope with the security issue in VANETs. Wei et al have incorporated the direct interactions and recommendations to evaluate and update the trust level of vehicles. Another similar trust based scheme for location finding has been proposed in (Soni et al., 2015). This scheme stands also on direct interactions and recommendations to validate or deny the presence of a desired location.

Other models have incorporated both of the reputation and similarity to assess the vehicle's trustworthiness. In (Hu et al., 2015), Hu et al have proposed the VTrust model to ensure a robust relay selection in VANETs. This framework stands on the global reputation value, direct previous experiences, recommendations and similarity score between the target and the message. However, Hu et al have not detailed the adopted method for the similarity assessment. Differently, Yang and Al Falasi et al have been more interested by the similarity assessment (Yang, 2013)(Al Falasi and Mohamed, 2015). Yang has presumed that the reputation of a new vehicle depends on the reputation of similar vehicles that have reported the same event and the similarity level between the reporter and these vehicles. Besides, he has supposed that evidences should be structured according to the reputation of both of the recommender and the sender and further on the similarity level between the evaluator and the recommender. Al Falasi et al have also adopted the similarity to evaluate the trust relationship between vehicles. They have assumed that the more vehicles behave similarly, the more they trust each other. Additionally, they have focused on the behavior assessment to supervise the vehicle's attitude in regard to the expected one. Li and Song have been also interested in the behavior assessment in order to build the entity's reputation and to detect the misbehaving nodes (Li and Song, 2016).

Many other models have adopted the similarity notion between messages instead of the similarity between the groups of vehicles to detect the wrong events. Mazilu et al have used similarity to find out the coincidence between the received trust index (encapsulated on the received message) and the previous ones (locally stored) that are related to messages reporting the same event (Mazilu et al., 2011). Zaidi et al have adopted the similarity to compare their own measurements with the others' detections in term of the speed, density and flow (Zaidi et al., 2014). The correlation between these criterions enables a vehicle to estimate the real traffic state and to detect the emergent situations. A framework for smart signal traffic control has been presented in (Płaczek and Bernas, 2016). It intends to detect the malicious data by incorporating the behavior and the similarity assessment.

Raya et al have also assessed the similarity between messages reporting the same event in order to distinguish between false and real events (Raya et al., 2008). They have focused on the data trust establishment in ephemeral ad hoc networks. To assess each message's trustworthiness, they have incorporated (1) the correlative trustworthiness of the event and its reporter, (2) the security status to discriminate between legitimate and illegitimate entities and (3) the proximity in terms of the time and location. As well, Yao et al have been based on the utility theory to combine the correlative trustworthiness of the event and its reporter and both of the time and location (Yao et al., 2017). Besides, they have further focused on the rep-

utation of the entity that has reported the message. Similarly, (Oluoch, 2015), Oluoch has almost adopted the same methodology to assess the data trustworthiness. He has assumed that the message value depends on the role and the reputation of its reporter, time and location.

The discussed trust management models are not self-adaptively adjusted to cope with the requirements of each kind of application. Some of them have been proposed to deal with the overall applications' classes by the same way while the others have been restricted to a particular type of application such as location finding, traffic jams, etc. Moreover, it is obvious that trust cannot only stand on the reputation assessment especially in ephemeral networks due to the high dynamicity of the network topology. Therefore, unlike other solutions, we propose a self-adaptive trust model that assumes that the decision-making differs not only from one application to another but also from one situation to another. Our aim is to enhance the security of the provided information, reduce the energy consumption and ensure a fast delivery of the reported event message.

3 OVERVIEW

VANET is a highly dynamic network that includes fast moving vehicles. These vehicles can meet only once to exchange information during a limited period. Accordingly, trust evaluation cannot only stand on the reputation assessment. It has to consider other concepts such as behavior and similarity assessment. Figure 1 depicts concepts and attributes that may interfere to ensure an effective and accurate decision-based trust assessment.

In this paper, we propose a self-adaptive trust model that aim to improve the decision making process. The next conceptual diagram (2) depicts the different processes that allow a vehicle to make its decision. We assume that it is not always required to execute all of these processes. Therefore, the decision-making may differ from one situation to another depending to the available information.

Whenever a vehicle or RSU receives a message it starts by checking its validity. Each event may last for a limited period. Thus, if the received message is not valid anymore, then it will be discarded. Otherwise, the establishment of the decision-making will depend on the next processes.

Reputation Assessment. Whenever a vehicle V_i receives a message from a nearby vehicle V_j, it can firstly check its reputation either locally (due to past interactions between them) or from an RSU. However, in highly dynamic networks, past interactions do not always exist. Therefore, if V_i have no past interactions with V_j (strange) then, we suppose that the type of this latter (e.g. police car, bus, etc.) may reflect its trust level. Nonetheless, if V_i has enough information on the reputation of V_j (familiar) then, it may decide whether to trust the received message or not.

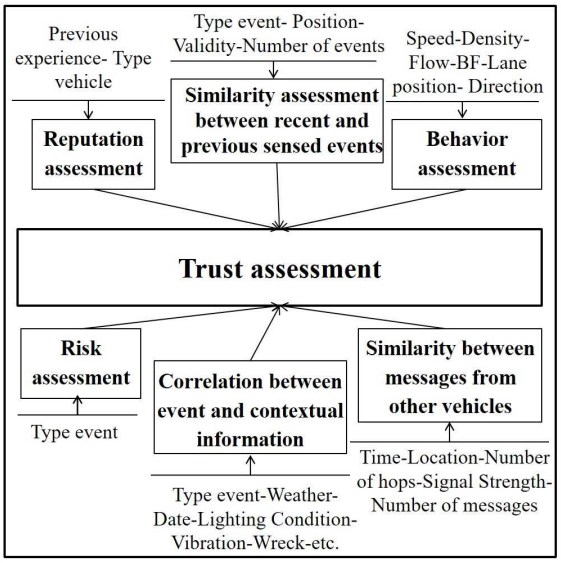

Figure 1: Representation of the required concepts and attributes for trust assessment.

Similarity Assessment between Recent and Previous Sensed Events. V_i can compare the recent received event with the previous sensed ones at the same position. In VANET, some events may last for a long period (days up to weeks) such as a working zone whereas other events have a short validity such as an accident. Based on the validity, the position and the number of similar previous events, V_i may estimate the feasibility of the recent received one.

Similarity Assessment between Messages. V_i can investigate the similarity between all of the received messages based on a set of attributes. The time and location denotes respectively when and where the event has been reported. The higher the number of similar messages in terms of time and location, the better the decision is. Besides, the message passes through a number of intermediate hops (NH) that may point out the likelihood of being threatened. Accordingly, the similarity assessment between messages in term of NH allow us to identify the more risky ones. Moreover, similarity between messages can be established based on the signal strength of each received message. If V_i detects any similar signal strengths then, it can decide that messages belong to the same entity that may present itself under different identities and different positions.

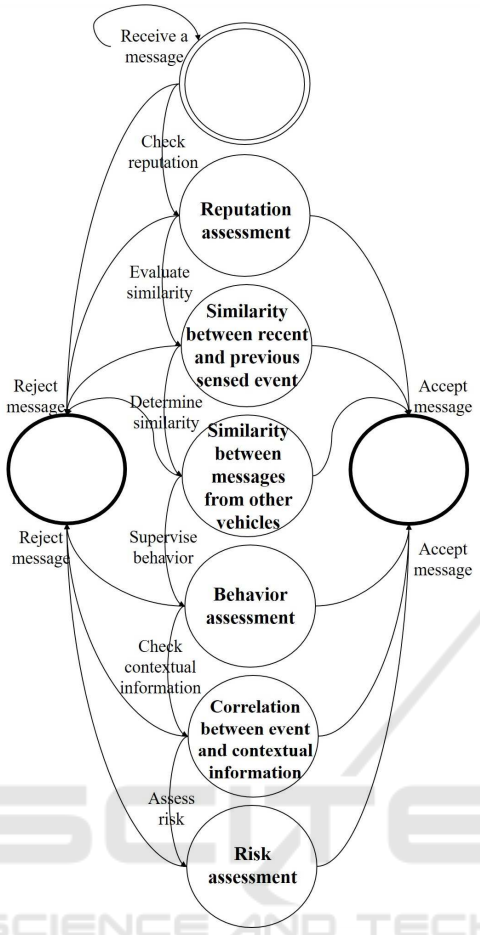

Figure 2: Conceptual Diagram for decision-making based on reputation, behavior and similarity assessment.

Behavior Assessment. V_i can evaluate the behavior of V_j based on a set of attributes such as speed, Breaking Frequency (BF), etc. For example, if V_j warns V_i about an accident on the lane L_1 then V_i may supervise the behavior of V_j versus the received alert and with respect to its direction. If V_j belongs to the accident direction and it keeps moving with the same speed or on the same lane (L_1) then V_i may decide that V_j misbehaves. Besides, if the speed of V_j mismatches with the density and the flow then, V_i discards the received alert. Moreover, the BF may play an important role to supervise the behavior of V_j. In emergent situations, this attribute may prove the existent of a risk especially in highways where the BF is usually low.

Correlation between the Event and Contextual Information. V_i can check the correlation between the received event and any contextual information such as vibration detection for accident alert, the weather (foggy, snowy, etc.), the date (holidays, weekend, etc.), lighting conditions, etc. For example, if Vi receives the message 'slippery road' and it detects that there is a dangerous turn ahead, there is no lights and it is raining then, it can believe the warning message and slow down.

Risk Assessment. If the driver cannot make a decision based on all of the previous alternatives then, it can choose to assess the risk of believing or denying the received message. On the one hand, for comfort applications such as searching for parking packs, if V_i receives a message that indicates that there is no free spaces and it cannot ensure that this alert is accurate then, it may decide to look for a space by itself. On the other hand, in critical applications such as accident warning, V_i may analyze the consequences of considering or denying the alert in both sides to decide whether to follow the same road or to change it.

In this section, we have shown that our proposal starts by locally estimating the credibility of the reported event (reputation, similarity between recent and previous sensed events). The aim behind this scheduling is to reduce both of time and energy consumption while preserving the accuracy of the decision-making. Moreover, this model can meet with the specifications of each class of applications. Safety applications require high accuracy and fast decision-making to disseminate the alert. Therefore, whenever a vehicle get sufficient information about the alert trustworthiness, it may not run the remaining processes and decide to broadcast the message to nearby vehicles. Regarding the comfort applications, they are not restrictive as the previous class. Usually, they do not require high security and accuracy.

4 CASE STUDY

In this section, we present the following scenario to investigate the benefit of our model in a real life case as depicted in Figure 3. This latter does not report real distances between different vehicles. It is only proposed to give an overall idea about the dissemination of an alert. We have assumed that an accident has occurred in a highway between two vehicles due to the excessive speed (V_1 and V_2 have been entirely damaged). Thus, the nearest vehicle V_3 can estimate the position of the accident based on the embedded sensors. Accordingly, the quality of these sensors has to be assessed so as to detect any deficiency in terms of timeliness, accuracy, etc. Subsequently, V_3 has to evaluate its own trustworthiness by itself based on the quality of its own measurements. Thereafter, it has to decide whether to broadcast the alert to its adjacents or not. In this case study, we assume that the dissemination of the accident warning message can be described as follows.

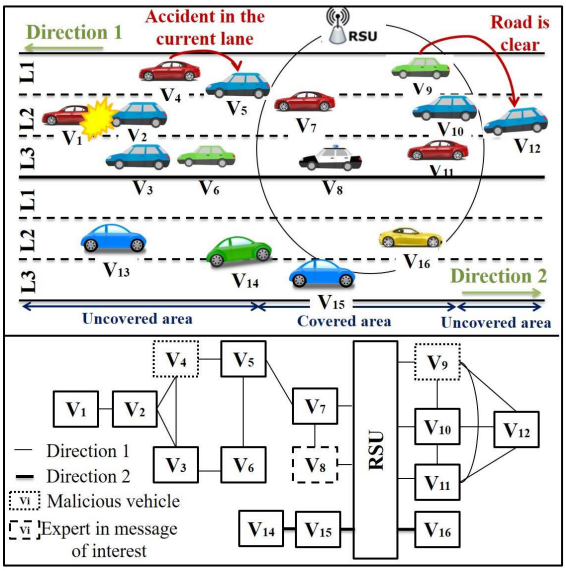

Figure 3: Graphic representation of the dissemination of an accident warning in a highway.

1. When V_4 receives the alert from V_3, it perceives that it also belongs to the transmission range of V_2 but it did not receive any alert from its side. According to our proposal, V_4 starts by checking if it has any previous interactions with V_2 and V_3. However, these vehicles are met for the first time. Thus, reputation assessment is not enough to make the appropriate decision. Thereafter, V_4 verifies if it has detected any similar previous events for the same position. Nonetheless, an accident remains valid only for a short period. Moreover, V_4 cannot stand on the similarity assessment between messages given that it has received only one message. Afterwards, V_4 can supervise the behavior of both of V_2 and V_3. It realizes that V_2 is not moving anymore while V_3 slows down due to the existence of some broken glass in its lane. Consequently, V_4 may ensure that the received alert is trustworthy. It decides to broadcast the alert but to lie about the lane of the accident. Similarly, V_6 decides to accept the warning message based only on the behavior assessment of V_3.

2. V_5 receives an accident warning message from V_4 and V_6. It detects that there is a conflict regarding the lane of the accident. Similarly, we assume that (1) the reputation assessment, (2) the short validity of the event and (3) the similarity assessment between messages do not allow V_5 to identify the malicious vehicle. Afterwards, V_5 remarks that V_6 and V_4 keep moving respectively in L_3 and L_1 and V_6 slows down (because V_3, the vehicle ahead, slows down) while V_4 keeps moving with the same speed. Consequently, it may deduce that V_4 is malicious because it did not slow down and further it did not change the lane if L_2 is really free. Therefore, V_5 decides to keep moving in the same lane, and to broadcast the message received from V_6.

3. V_7 receives the alert only from V_5. V_7 belongs to the transmission range of the RSU. It requests the reputation of V_5 from the RSU. We assume that the (1) recovered reputation, (2) the similarity between recent and local previous events and (3) the similarity between other received messages do not allow V_7 to decide whether to trust the alert or not. Thereafter, V_7 tries to inspect the behavior of V_5. It detects that V_5 keeps moving with the same speed and on the same lane which is different from the lane of the accident. Based only on these information, V_7 cannot believe that the accident exists. Afterwards, V_7 looks for any contextual information that can prove the accident alert. We assume that V_7 cannot observe any contextual information. Therefore, it decides to assess the consequences of believing in the received warning or not based on the event type. Therefore, it decides to trust the alert and to move from L_2.

4. V_7 and V_8 have high reputation values (V_8 is expert in message of interest). Thus, the RSU trust the warning message reported by V_7 and V_8 and it decides to broadcast it to the other covered vehicles (V_9, V_{10} and V_{11}). All of these vehicles trust the alert. However, V_9 decides to lie about the traffic state. The RSU may perceive that V_9 is malicious and it decides to reduce its reputation value.

5. V_{12} belongs to the transmission range of V_9, V_{10} and V_{11}. It receives three warning messages at near time. V_9 says that the road is clear whereas V_{10} and V_{11} say that there is an accident. We assume that V_{12} has no past experiences with the three previous vehicles. As well, it cannot rely on the similarity assessment between the recent and the previous sensed events. Thereafter, V_{12} checks the similarity between all of the received messages. It realizes that both of V_{10} and V_{11} report the same time and the same location of the accident. Besides, V_{10} and V_{11} have different signal strengths which mean that there is no Sybil attack. Accordingly, V_{12} decides to accept the accident warning message.

This scenario shows that our proposed adaptive trust model may perform well to identify vehicles that misbehave such as fake information attack, drop message attack, Sybil attack and collusion attack. Besides, this model can reduce the energy consumption since it does not require recommendations from third

parties. We have also shown that whenever a vehicle get sufficient information about the alert trustworthiness, it may not run the remaining processes. This fact may accelerate the decision-making process especially for time-critical applications.

5 CONCLUSIONS

This paper proposes a self-adaptive trust model for VANETs. This model intends to handle with the specifications of each class of applications in a different manner. The aim of our proposal is to enhance the decision-making process, minimize both time and energy for decision-making and improve the network's security. We have applied this model on a real life case to evaluate its performance and to show its benefits. In the future, we plan to detail this proposal and further to identify the appropriate techniques to estimate the accurate trust value. Besides, we plan to pay more attention to the quality of raw sensed data in order to preserve the quality of the provided applications. Finally, we have to investigate and validate the efficiency, scalability, robustness and overhead of this model.

ACKNOWLEDGEMENTS

This work was supported by the PHC Utique program of the French Ministry of Foreign Affairs and Ministry of higher education and research and the Tunisian Ministry of higher education and scientific research in the CMCU project number 16G1404.

REFERENCES

Al Falasi, H. and Mohamed, N. (2015). Similarity-based trust management system for detecting fake safety messages in vanets. In *International Conference on Internet of Vehicles*, pages 273–284. Springer.

Campolo, C., Molinaro, A., and Scopigno, R. (2015). Vehicular ad hoc networks. *Standards, Solutions, and Research*.

Dwivedi, S. and Dubey, R. (2016). Review in trust and vehicle scenario in vanet. *International Journal of Future Generation Communication and Networking*, 9(5):305–314.

Hu, H., Lu, R., and Zhang, Z. (2015). Vtrust: a robust trust framework for relay selection in hybrid vehicular communications. In *Global Communications Conference (GLOBECOM), 2015 IEEE*, pages 1–6. IEEE.

La Vinh, H. and Cavalli, A. R. (2014). Security attacks and solutions in vehicular ad hoc networks: a survey. *International journal on AdHoc networking systems (IJANS)*, 4(2):1–20.

Li, W. and Song, H. (2016). Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 17(4):960–969.

Mazilu, S., Teler, M., and Dobre, C. (2011). Securing vehicular networks based on data-trust computation. In *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2011 International Conference on*, pages 51–58. IEEE.

Oluoch, J. O. (2015). *A unified framework for trust management in Vehicular Ad Hoc Networks (VANET)*. PhD thesis, Oakland University.

Płaczek, B. and Bernas, M. (2016). Detection of malicious data in vehicular ad hoc networks for traffic signal control applications. In *International Conference on Computer Networks*, pages 72–82. Springer.

Raya, M., Papadimitratos, P., Gligor, V. D., and Hubaux, J.-P. (2008). On data-centric trust establishment in ephemeral ad hoc networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages 1238–1246. IEEE.

Soleymani, S. A., Abdullah, A. H., Hassan, W. H., Anisi, M. H., Goudarzi, S., Baee, M. A. R., and Mandala, S. (2015). Trust management in vehicular ad hoc network: a systematic review. *EURASIP Journal on Wireless Communications and Networking*, 2015(1):146.

Soni, S., Sharma, K., and Chaurasia, B. K. (2015). Trust based scheme for location finding in vanets. In *Advances in Optical Science and Engineering*, pages 425–432. Springer.

Wei, Z., Yu, F. R., and Boukerche, A. (2014). Trust based security enhancements for vehicular ad hocnetworks. In *Proceedings of the fourth ACM international symposium on Development and analysis of intelligent vehicular networks and applications*, pages 103–109. ACM.

Yang, N. (2013). A similarity based trust and reputation management framework for vanets. *International Journal of Future Generation Communication and Networking*, 6(2):25–34.

Yao, X., Zhang, X., Ning, H., and Li, P. (2017). Using trust model to ensure reliable data acquisition in vanets. *Ad Hoc Networks*, 55:107–118.

Zaidi, K., Milojevic, M., Rakocevic, V., and Rajarajan, M. (2014). Data-centric rogue node detection in vanets. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on*, pages 398–405. IEEE.

Zhang, J. (2011). A survey on trust management for vanets. In *Advanced information networking and applications (AINA), 2011 IEEE international conference on*, pages 105–112. IEEE.