

An Infrastructure-Based Trust Management Framework for Cooperative ITS

Rihab Abidi^{1,4}, Nabil Sahli², Wassim Trojet³, Nadia Ben Azzouna¹ and Ghaleb Hoblos⁴

¹University of Tunis, ISG, SMART Lab, Av. de la Liberte, Tunis, Tunisia

²Computer Science Department, German University of Technology (GUTech), Muscat, Oman

³Higher College of Technology UAE, Abu Dhabi, U.A.E.

⁴Normandy University, UNIROUEN, ESIGELEEC, IRSEEM, Av. Galilee, Normandie, France

Keywords: Intelligent Transportation System, Trust Management, Infrastructure-Based Architecture.

Abstract: Intelligent Transportation Systems (ITSs) have been exploited by developed countries to enhance the quality of transportation services. However, these systems are still facing major bottlenecks to be addressed such as the data density, precision and reliability of perceived data and computational feasibility of the nodes. Trust management is a mechanism applied to secure the vehicular networks. However, most of the proposed trust models that are applied to Vehicular Ad-hoc NETWORK (VANET) do not address all the aforementioned challenges of ITS. In this paper, we present a comprehensive framework of trust management specifically designed for ITS applications. The proposed framework is an infrastructure-based solution that relies on Smart Road Signs (SRSs) to assess the trustworthiness of traffic data and nodes of the network. The idea of the framework is to use autonomous SRSs that are able to collect raw data and evaluate it in order to alert the drivers with reliable traffic information in real time. We adopt a hierarchical architecture that exploits a two-level trust evaluation to ensure accuracy, scalability, security and high reactivity of ITS applications. A discussion of the framework and its strengths is presented.


1 INTRODUCTION


With the growth of traffic volume, the modern society faces major transportation challenges that may cause serious and harmful consequences, such as accidents, congestions, environmental consequences and even economic impacts. Intelligent Transportation Systems (ITSs) are a promising solution that helps improve the traffic management by deploying sustainable and innovative platforms (Guerrero-Ibanez et al., 2015).


Despite its development over the last decade, the ITS field still faces some challenges and bottlenecks, mainly, precision, security and computational issues (Lin et al., 2017). Traditional solutions that are based on Public Key Infrastructure (PKI) are not able to se-


cure the network from legit nodes that could disturb the network and send untrustworthy data. Trust management models are thus used to secure the network and evaluate the precision and relevance of the shared data. In fact, trust management models refer to the evaluation of the accuracy and relevance of a trustee node or data by a trustor node using quantified beliefs in order to mitigate and reduce the impact of attackers (Hbaieb et al., 2022).


In this regard, we propose a trust framework to support the ITS applications. We propose an infrastructure-based solution that uses Smart Road Signs (SRSs) for cooperative ITS. Several architectures of SRSs have been proposed in the literature. For instance, the project proposed in (Czyżewski et al., 2019) is based on intelligent road signs to manage the road traffic and prevent highway collisions. The intelligent road signs are able to collect data from sensors and exchange it, using LTE and LoRa WAN technologies. However, while dynamic message signs (DMSs) are employed in different countries, these DMSs remain passive and display traffic

^a <https://orcid.org/0000-0002-6108-7854>

^b <https://orcid.org/0000-0002-9805-6859>

^c <https://orcid.org/0000-0001-7792-4402>

^d <https://orcid.org/0000-0002-6953-2086>

^e <https://orcid.org/0000-0003-3268-5270>

information issued from traffic management centers. In this framework, we rely on the SRSs to take advantage of their intelligence which lies in their autonomy, proactivity and their ability to process data without the intervention of third parties (Hamdani et al., 2022). The aim of the proposed framework is to use autonomous and SRSs that collect real-time data from different sources and collaborate to evaluate its trustworthiness.

Researchers proposed several trust models for Vehicular Ad-hoc NETWORK (VANET). However, most trust models cover at most few challenges of the ITS applications. In fact, studies show that achieving the optimal performance of ITS applications lies in combining several characteristics and requirements. Mainly, the ITS applications are meant to provide accurate information in real-time performance while managing the message overheads and ensuring the security and privacy of the network (Ben Hamida et al., 2015).

To the best of our knowledge, there is no model that meets the most crucial requirements of the ITS, namely, accuracy, scalability, security, reactivity, and privacy.

In this context, we propose a comprehensive framework of a trust management model that enhances the performance of ITS applications. The aim of the proposed framework is to evaluate the trustworthiness of reported traffic events and the data sources. Our aim is to ensure that the trust model responds to the crucial requirements of ITS at once. In fact, we exploit multi-sourcing of traffic-related data to ensure the overall visibility of the environment. These data may be sensed from different transportation nodes such as vehicles, travellers, infrastructure and even social media. Moreover, we adopt a decentralized architecture to reduce the communication and computation overhead.

The rest of the paper is organized as follows. Section 2 presents the related works. Section 3 introduces the network model. Section 4 describes the proposed framework. We discuss the design goals in section 5. Section 6 concludes the paper.

2 RELATED WORKS

Different trust models have been proposed to evaluate the trustworthiness of traffic data and/or nodes. Generally, researchers review the proposed trust model according to the subject of trust: entity-centric, data-centric, and hybrid models. In this paper we focus on the addressed requirements of the trust model.

For instance, Bhargava and Verma propose in

(Bhargava and Verma, 2022) trust management model which ensures accuracy and security requirements. In fact, the authors consider the uncertainty of the data to increase the precision. They use Dempster-Shafer theory (DST) to aggregate direct and indirect trust of the vehicles. In order to increase the precision of the trust evaluation, the authors use contextual information to define the type of the messages that are attacked by the malicious vehicles. The considered messages are Lane Change warning (LCW), Stopped Vehicle Warning (SVW), and Emergency Brake warning (EBW). Moreover, the authors use additional functions to enhance the precision of the trust evaluation and boost the security of the model. The used functions are the *penalty*, the *forgetting*, the *rewarding*, and the *forgiving functions*.

Forgetting function is also used in (Zhang et al., 2020b) by Zhang et al. and it is introduced with a decay factor to cope with the On-Off attacks (OOA) and the Newcomer attacks (NA). The idea of using these factors is to prevent the quick increase of the trust value of the nodes. This technique helps to encourage the nodes to present a good behaviour in order to maintain their trust values. In addition, the authors take advantage of the contextual information about the vehicles, such as *vehicle type*, *vehicle age*, *braking performance*, *handling stability*, etc. and the drivers' characteristics to achieve the accuracy requirement of the trust evaluation.

The security and privacy requirements are tackled by Ahmed et al. in (Ahmed et al., 2022). The authors use the blockchain technology to check the legitimacy and authenticity of the nodes joining the network. The new nodes that join the network for the first time are registered in the blockchain by the Trusted Authority. Then, the Road Side Units (RSUs) evaluate the trustworthiness of the vehicles and add their updated trust values to the blockchain ledger.

Zhang et al. in (Zhang et al., 2020a) consider the accuracy, the security and the reactivity of their trust model. They propose a learning approach that uses a Feedforward Neural Network algorithm (FNN) to estimate the local and global trust values. They use several contextual information as an input to the FNN, such as the type, the location of the traffic incident, and location of the reporting vehicle. The proposed model is designed to cope with Bad Mouting attack (BMA), On-Off Attack (OOA), and Simple Attack (SA). In fact, the authors combine the deep learning technique with the blockchain technology to learn the correlation between the malicious nodes and to predict their behaviour. Moreover, the blockchain is used to enhance the security by checking the authenticity of the vehicles and the reported events. The

blockchain is managed by the RSUs instead of the vehicles in order to ensure the scalability of the model.

Gazdar et al. in (Gazdar et al., 2022) take advantage of the blockchain technology to enhance the security of the vehicular network. The authors consider mainly the BMA. Indeed, they affirm that the features of the blockchain ensure the data integrity and availability. Moreover, they address the cold start problem by assigning an initial value to the new nodes that join the network and saving their updated trust values in the blockchain ledger. The authors consider also the reactivity requirement to cope with time-sensitive applications. In fact, they employ a lightweight tier-based technique to compute the trustworthiness of vehicles in order to reduce communication overhead (Alboqomi et al., 2020).

A decentralized trust model is proposed by Chen et al. in (Chen et al., 2020). The authors use an incentive mechanism to encourage nodes to participate in the trust management process, thus increasing the accuracy of the trust evaluation. Hence, the nodes are either rewarded or punished based on the quality and the workload of their contribution. Moreover, the incentive mechanism helps the model to cope with the BMA by encouraging the nodes to be honest. Moreover, vehicles encrypt and sign exchanged data using a unique and a unique key pair in order to cope with the Sybil attack (SyA). The proposed model considers also the reactivity and scalability requirements by designing a hierarchical architecture to reduce the latency of the model. In fact, the authors employ a decentralized consensus mechanism executed on two layers in a parallel manner: the transaction validation and the block verification and consensus.

Guo et al. propose a trust model in (Guo et al., 2020) that cope with malicious attacks. The proposed model addresses mainly the accuracy requirement. The authors use the Reinforcement learning to dynamically adjust the trust evaluation strategy based on the scenario. Thus, they employ contextual information such as *time of event occurrence* and *location of the event*. The trust information based on internal information (direct sensing and self-experience information) and external information (information reported by other entities).

As presented in table 1, the beforementioned trust management models consider, at most, one or few requirements of the ITS applications. For instance, few works consider only the accuracy and security requirements, such as in (Li and Song, 2015), and (Zhang et al., 2020b), while (Bhargava and Verma, 2022) consider also the reactivity. Moreover, we noticed that the accuracy and security requirements are the most considered among the addressed require-

ments. To the best of our knowledge, there is not a general trust model that considers all the requirements at once. However, the mentioned requirements are crucial for ITS applications. In particular, accuracy and security are critical requirements, especially for congestion control applications (Alam et al., 2016), (Ben Hamida et al., 2015). Indeed, the diffusion of erroneous information, due to inaccuracy of raw data or attacks by malicious nodes, may cause severe consequences such as high congestion or even road accidents. High reactivity is also a key requirement for time sensitive applications. In case of congestion, the drivers should be alerted in real-time to avoid traffic bottlenecks. Therefore, we propose a generic framework of a trust model that may be used by ITS applications. The aim of this work is to provide a trust framework that fulfils all the crucial requirements of the ITS applications in order to enhance the provided services.

3 OVERVIEW

The proposed framework relies on a hierarchical infrastructure-based vehicular network where the smart road signs are the core components. This architecture enables a real-time dissemination of traffic information and monitoring of the Intelligent Transportation Systems.

First, we consider that the traffic roads are partitioned into smaller regions, as shown in figure 1.

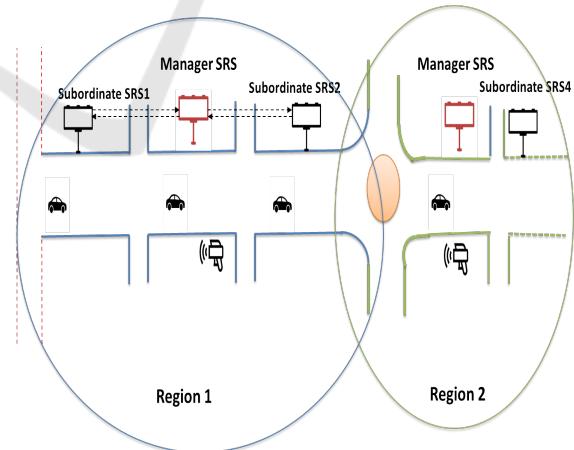


Figure 1: Region-based vehicular network.

Each region is a set of connected roads that encompasses several nodes that manage the traffic information in these roads. Nodes include smart road signs (SRS) as well as traffic/environment data sources. Smart road signs can be Manager or Subordinate as defined in (Sahli et al., 2022) as Master and Slave.

Table 1: The considered requirements of the surveyed trust models.

Paper	Accuracy	Security	Reactivity	Scalability	Privacy
(Bhargava and Verma, 2022)	✓	✓			
(Zhang et al., 2020b)	✓	✓			
(Ahmed et al., 2022)		✓			✓
(Zhang et al., 2020a)	✓	✓	✓		
(Gazdar et al., 2022)	✓	✓	✓		
(Chen et al., 2020)	✓	✓	✓	✓	
(Guo et al., 2020)	✓	✓			

A Manager SRS is in charge of collecting data from Subordinates. Each region includes many subordinates and one Manager. Data sources can be connected vehicles, surveillance cameras, radar, etc. Let us consider a region composed of one manager SRS, n subordinates, and m data sources. In particular, when a road is congested the data sources alert the nearest SRSs about the traffic state. Hence, the subordinate SRSs evaluate the trustworthiness of the reported event and alert the drivers about possible traffic congestion. The evaluations of the subordinate SRSs are then transmitted to the manager SRS to aggregate them. The final warning message will be sent to the subordinate SRSs to update the displayed alert messages.

Figure 2 presents the general architecture of our network system and the dissemination of the data flow. In what follows, we present the major components of our framework.

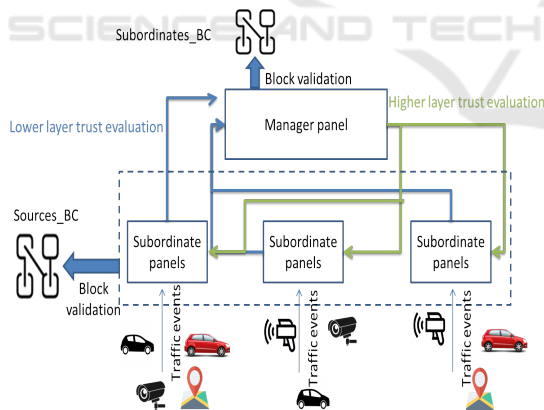


Figure 2: General architecture of the trust model.

1. SRSs: The SRSs are the main component in the network model. They are equipped with digital screens to alert drivers about the traffic state in real-time (Sahli et al., 2022). These SRSs are connected to the internet and endowed with processing capabilities. Accordingly, they are able to collect traffic-related data and evaluate their credibility, in order to estimate and communicate the traffic state. Unlike the existing DMSs, which

display the traffic state estimated by traffic management centers, the SRSs are endowed with intelligence and autonomy allowing them to process the sensed data without human intervention. We adopt a hierarchical architecture based on two types of SRSs:

- (a) Manager SRSs: These SRSs are assumed to be fully trusted by the neighbouring subordinate SRSs. We suppose that the manager SRSs are secured and equipped with higher storage and communication capabilities. The main role of manager SRSs is to aggregate the evaluations of subordinate SRSs about the reported traffic events. In general, the manager SRS controls the subordinates localized in its region. Accordingly, it evaluates and updates their trust values and stores them in the *Subordinates-BC* blockchain. In fact, the *Subordinates-BC* is used to keep track of the trustworthiness of the subordinates.
- (b) Subordinate SRSs: Unlike the manager SRSs, we suppose that the subordinate SRSs may be compromised. Hence, their credibility is evaluated by the manager SRSs. However, they are responsible for the evaluation of the trustworthiness of the traffic events reported by the data sources and updating the values of their trust values. As shown in figure 2, the subordinate SRSs contribute to the block validation to update the trust values of the data sources in the *sources-BC* blockchain.

2. Data sources: Data sources are a set of mobile nodes, such as connected vehicles, and static nodes, like surveillance cameras, radars, pneumatic tube sensors, and inductive loops. These nodes are responsible for reporting traffic events to the subordinate SRSs. The data sources may communicate erroneous data due to physical failure or intentionally when hijacked by malicious attackers.

4 DETAILED DESIGN

In this section, we present the detailed design of the proposed framework. In fact, the proposed model is composed of five main modules:

1. Events classification
2. Lower layer trust evaluation
3. Higher layer trust evaluation
4. Reward/ punishment
5. Blockchain validation

4.1 Events Classification

We suppose that traffic event messages are sent to the nearest subordinate SRS. Those messages will be classified into groups of events according to spatio-temporal information and semantic analysis. The idea of the event classification module is to assemble the messages that report the same event. Moreover, the *event classification* module assigns a severity degree to each group of event according to the frequency of the reports and the type of the event. Therefore, the group of events with the highest severity degree will be processed before the group of events with a lower severity degree. For instance, the module will pay more attention to events of type “accidents” than events of type “light congestion”. The aim is to increase the reactivity of the model in the presence of various traffic events and to avoid serious consequences.

4.2 Lower Layer Trust Evaluation

The proposed framework uses the data reported by several data sources in order to increase the visibility of the surrounding environment. However, the data sources may be compromised and intentionally provide erroneous data, or unintentionally in case of physical failure. Accordingly, a trust evaluation method will be used by the subordinate SRSs to estimate the trustworthiness of the provided data and/or the node that reported it. Several trust methodologies proposed in the literature may be used. For example, plausibility checking using fuzzy logic may be a suitable approach to evaluate both the data and the node trustworthiness such as in (Souissi et al., 2022). Other methodologies such as game theory and belief theory, and regression analysis also may be used to estimate the trustworthiness of the provided data (Wang et al., 2016), (Chen et al., 2016), (Kang et al., 2018).

4.3 Higher Layer Trust Evaluation

The final decision on whether to choose to trust or ignore the reported events is made by the manager SRS. Therefore, the manager SRS estimates the overall trust out of the evaluation of the subordinate SRSs in the same region. Moreover, a manager SRS may collaborate with nearby manager SRSs to estimate the trustworthiness of events occurring on the edges of its regions. The idea behind adding a second evaluation of the reported events is that the manager SRS has a general overview of the environment by combining the estimations of the subordinate SRSs. Different approaches may be used for the trust formation. For example, static weighted sum and dynamic weighted sum may be used to combine the trust evaluation of the subordinate SRSs.

4.4 Reward/ Punishment

The reward/punishment module is proposed to be applied at two levels. At the higher layer, it is implemented in the manager SRS in order to adjust the trustworthiness of the subordinate SRSs. At the lower layer, it is deployed in the subordinate SRS to adjust the behaviour of the data sources and to boost their cooperativeness.

4.5 Blockchain Validation

We propose to add two blockchain modules to save and track the behaviour of the nodes in the network. The first blockchain is used to save the trustworthiness of the data sources. This ledger is shared between the subordinate SRSs. The second blockchain is used to store the trustworthiness of the subordinate SRSs. The second ledger is controlled by the manager SRS.

The use of the blockchain technology ensures the integrity of the saved data, hence increases the data reliability. Different consensus mechanisms may be used in this regard. In particular, Proof-of-stake (PoS), is an efficient mechanism in terms of energy. Other mechanisms such as Delegated Proof of Stake (DPoS), Proof of Work (PoW), and Proof of Authority (PoA) may be also used (Liu et al., 2019), (Chen et al., 2020), (Gazdar et al., 2022).

The overall workflow of the trust framework is shown in figure 3. Hereafter, we list the sequence of steps performed by the framework.

1. The data sources report an event
2. The *event classification* module classifies the reported events into groups

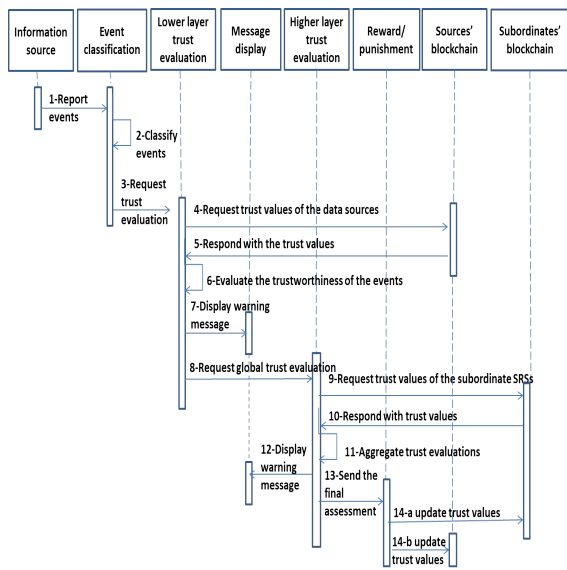


Figure 3: Component interaction diagram of the proposed framework.

3. The *lower layer trust evaluation* module receives the group of events to evaluate their trustworthiness
4. The *lower layer trust evaluation* module requests the trust values of the data sources from the blockchain
5. The *lower layer trust evaluation* module receives the necessary data from the blockchain
6. The *lower layer trust evaluation* module estimates the trustworthiness of the reported event
7. The alert message is then sent to be displayed on the SRSs
8. The assessments of the subordinate SRSs are sent to the *higher layer trust evaluation* module to aggregate their evaluations
9. The *higher layer trust evaluation* module requests the trust values of the salve SRSs from the blockchain ledger
10. The *higher layer trust evaluation* module receives the necessary data from the blockchain
11. The *higher layer trust evaluation* module executes the final trust evaluation of the reported event using the assessments of the subordinate SRS
12. The displayed alert message is updated according to the final evaluation of the *higher layer trust evaluation* module
13. The final trust assessment is then sent to the *reward/punishment* module to evaluate the trustworthiness of the data sources and the subordinate SRS

- 14.(a) The reward/punishment module updates the trust values of the subordinate SRSs and sent it to be saved in the blockchain ledgers
- (b) The reward/punishment module updates the trust values of the data sources and sent it to be saved in the blockchain ledgers

5 CASE STUDY

In this section, we present a case study to explain the dissemination and the process of event alert messages within the proposed framework. Figure 4 describes the discussed case study.

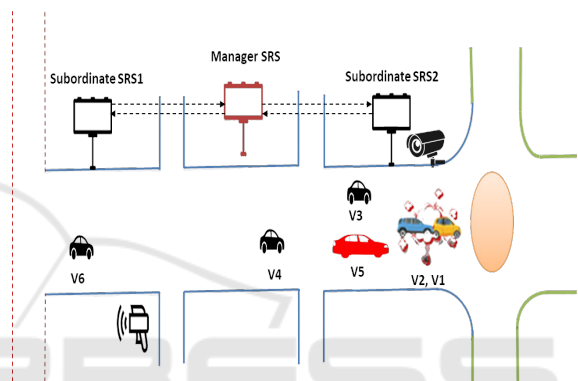


Figure 4: Representation of the case study scenario.

We suppose that the considered region is composed of a manager SRS, two subordinate SRSs, a surveillance camera, radar and six vehicles. In this context, we use the surveillance camera, the radar and the vehicles as our data sources. In this scenario, we suppose that an accident has occurred on a road transcend between two vehicles, V1 and V2. We suppose that vehicle V3 and V4 reported to the second SRS the occurrence of a crash event to SRS2. We suppose that V5 is a malicious node and reported to SRS2 that traffic flow is normal. We suppose also that the surveillance camera detected the presence of the accident and reported it to SRS2. Moreover, we suppose that vehicle V6 and the radar reported that there is a light congestion to SRS1. Hereafter, we describe the process of the evaluation of the alert messages.

1. The reported events will be classified into event groups using the spatio-temporal information and semantic analysis. Let us consider that V3, V4, V6, the radar and the surveillance camera sent the detected events approximately at the same time and neighbouring localization. Moreover, the module will identify that the light congestion may be related to the crash event. Accordingly, we will have two groups of events:

- E1 that combines the accident report by V3, V4, the surveillance camera and the light congestion by V6 and the radar.
- E2 that reports a normal traffic flow by V5.

The group of events E1 will be assigned the highest severity degree because it reports an event of type accident and has the highest number of reports. Accordingly, it will be processed in priority. Similarly, E2 will have the lowest severity degree.

2. SRS1 and SRS2 evaluate the trustworthiness of the reported events in E1 while considering the trustworthiness of the data sources stored in the blockchain.
3. A warning message will be then displayed on SRS1 and SRS2. Let us assume that the trust assessment of SRS1 of the event E1 is 0.7. Hence, the displayed message will be “70% chance that there is an accident ahead”. The idea is to increase the reactivity of the framework. Therefore, the drivers will be aware of the possibility of the presence of an accident, even before the final evaluation of the manager SRS.
4. The evaluations of SRS1 and SRS2 will be transmitted to the manager SRS to aggregate them, and provide the final trust value of the event while considering the trustworthiness of the subordinate SRSs that are registered in the blockchain.
5. The displayed messages will be updated after the final evaluation of the manager SRS.
6. The final evaluation of the manager SRS will be used to update the trustworthiness of the data sources and the subordinate SRSs.

6 PERFORMANCE ANALYSIS

In this section, we discuss the presumptions we considered in the design of the framework of the trust management framework to present its strengths.

1. **Presumption 1:** The proposed framework ensures the scalability of the trust model to follow the continuous growth of the ITS environment.
Discussion: The decentralized architecture of the framework will help to scale down the traffic overhead of the network. The partitioning of the road network into smaller regions limits the number of messages exchanged between the nodes of the network. Moreover, we propose an infrastructure-based architecture without internal communication between the data sources.
2. **Presumption 2:** The proposed framework increases the accuracy of the displayed traffic state.

Discussion: The multi-sourcing data fusion reduces the uncertainty of the environment observation. Moreover, the two-level trust evaluation scheme helps to have a global vision of the reliability of the reported traffic events. In the low evaluation layer we exploit the data provided by the data sources. In the upper evaluation layer we use the assessments of the subordinate SRSs.

3. **Presumption 3:** The proposed framework ensures the integrity, the availability, and the privacy of the data.

Discussion: The use of the blockchain technology ensures that the stored data is immutable. Blocks validation requires the validation of the majority of nodes to ensure the integrity of the information. The ledgers of the blockchain are replicated and synchronized, which avoids single-point failure. Therefore, it ensures the availability of the data. Moreover, blockchain ledgers can only be accessed by SRSs which protect sensitive data from being leaked.

4. **Presumption 4:** The proposed framework increases the reactivity of the ITS.

Discussion: The classification of the reported events and the evaluation of the severity of the events using the frequency of the reports and their types help to process the events of highest priority. Moreover, the decentralized and hierarchical architecture combined with the blockchain technology reduces the communication overhead (Gazdar et al., 2022). Hence, it reduces the response time of the ITS.

5. **Presumption 5:** The proposed framework of the trust model meets the requirements of the ITS applications.

Discussion: Due to the increasing number of the ITS components and to the time sensitivity of their applications, especially the traffic congestion management applications, the architecture of the ITS applications must be scalable, accurate and reactive to the changes of the environment. As discussed in the proposition above, the proposed framework would be scalable and able to provide accurate information in a short response time.

7 CONCLUSION

We propose in this paper an open framework for a trust management model to be enforced in ITS. The aim is to enhance the performance of ITS by ensuring its scalability, accuracy, security and the reactivity. We presented the general modules that should be

enforced and we discussed their efficiency and benefits. However, the proposed framework might be unsuitable for rural environments. We intend to further investigate and identify the appropriate techniques to be applied in each module. Besides, we intend to run validation experimentation to test the validity of the hypotheses.

REFERENCES

- Ahmed, W., Di, W., and Mukathe, D. (2022). Privacy-preserving blockchain-based authentication and trust management in vanets. *IET Networks*.
- Alam, M., Ferreira, J., and Fonseca, J. (2016). Introduction to intelligent transportation systems. In *Intelligent transportation systems*, pages 1–17. Springer.
- Alboqomi, O., Gazdar, T., and Munshi, A. (2020). A new blockchain-based trust management protocol for vehicular ad hoc networks. In *The 4th International Conference on Future Networks and Distributed Systems (ICFNDS)*, pages 1–5.
- Ben Hamida, E., Noura, H., and Znaïdi, W. (2015). Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures. *Electronics*, 4(3):380–423.
- Bhargava, A. and Verma, S. (2022). Duel: Dempster uncertainty-based enhanced-trust level scheme for vanet. *IEEE Transactions on Intelligent Transportation Systems*.
- Chen, X., Ding, J., and Lu, Z. (2020). A decentralized trust management system for intelligent transportation environments. *IEEE Transactions on Intelligent Transportation Systems*, 23(1):558–571.
- Chen, Y., Weng, S., Guo, W., and Xiong, N. (2016). A game theory algorithm for intra-cluster data aggregation in a vehicular ad hoc network. *Sensors*, 16(2):245.
- Czyżewski, A., Sroczynski, A., Śmiałkowski, T., and Hoffmann, P. (2019). Development of intelligent road signs with v2x interface for adaptive traffic controlling. In *2019 6th International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*, pages 1–7. IEEE.
- Gazdar, T., Alboqomi, O., and Munshi, A. (2022). A decentralized blockchain-based trust management framework for vehicular ad hoc networks. *Smart Cities*, 5(1):348–363.
- Guerrero-Ibanez, J. A., Zeadally, S., and Contreras-Castillo, J. (2015). Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies. *IEEE Wireless Communications*, 22(6):122–128.
- Guo, J., Li, X., Liu, Z., Ma, J., Yang, C., Zhang, J., and Wu, D. (2020). Trove: A context-awareness trust model for vanets using reinforcement learning. *IEEE Internet of Things Journal*, 7(7):6647–6662.
- Hamdani, M., Sahli, N., Jabeur, N., and Khezami, N. (2022). Agent-based approach for connected vehicles and smart road signs collaboration. *Computing and Informatics*, 41(1):376–396.
- Hbaieb, A., Ayed, S., and Chaari, L. (2022). A survey of trust management in the internet of vehicles. *Computer Networks*, 203:108558.
- Kang, J., Yu, R., Huang, X., Wu, M., Maharjan, S., Xie, S., and Zhang, Y. (2018). Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet of Things Journal*, 6(3):4660–4670.
- Li, W. and Song, H. (2015). Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE transactions on intelligent transportation systems*, 17(4):960–969.
- Lin, Y., Wang, P., and Ma, M. (2017). Intelligent transportation system (its): Concept, challenge and opportunity. In *2017 IEEE 3rd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, pages 167–172. IEEE.
- Liu, X., Huang, H., Xiao, F., and Ma, Z. (2019). A blockchain-based trust management with conditional privacy-preserving announcement scheme for vanets. *IEEE Internet of Things Journal*, 7(5):4101–4112.
- Sahli, N., Trojet, W., Zhang, Z., and Abdallah, N. O. (2022). Towards a network of dynamic message signs for congestion alerting. *Computing and Informatics*, 41(2):609–626.
- Souissi, I., Ben Azzouna, N., Abidi, R., Berradia, T., and Ben Said, L. (2022). Sp-trust: a trust management model for speed trust in vehicular networks. *International Journal of Computers and Applications*, 44(11):1065–1073.
- Wang, Y., Cai, Z., Yin, G., Gao, Y., Tong, X., and Han, Q. (2016). A game theory-based trust measurement model for social networks. *Computational social networks*, 3(1):1–16.
- Zhang, C., Li, W., Luo, Y., and Hu, Y. (2020a). Ait: An ai-enabled trust management system for vehicular networks using blockchain technology. *IEEE Internet of Things Journal*, 8(5):3157–3169.
- Zhang, J., Zheng, K., Zhang, D., and Yan, B. (2020b). Aatms: An anti-attack trust management scheme in vanet. *IEEE Access*, 8:21077–21090.