


# Infrastructure-Based Communication Trust Model for Intelligent Transportation Systems

Malek Lachheb<sup>1</sup><sup>a</sup>, Rihab Abidi<sup>1,2</sup><sup>b</sup>, Nadia Ben Azzouna<sup>1</sup><sup>c</sup> and Nabil Sahli<sup>3</sup><sup>d</sup>

<sup>1</sup>Université de Tunis, Institut Supérieur de Gestion de Tunis, SMART Lab, Av. de la Liberté, Tunis, Tunisia

<sup>2</sup>Normandy University, UNIROUEN, ESIGELEC, IRSEEM, Av. Galilee, Normandie, France

<sup>3</sup>Computer Science Department, German University of Technology in Oman (GUtech), Muscat, Oman

**Keywords:** Trust Model, Communication Trust, Infrastructure-Based Model, Smart Road Signs, Fuzzy Logic, Dempster Shafer Theory.

**Abstract:** Intelligent Transportation Systems (ITS) aim to enhance traffic management through Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) and Infrastructure-to-Infrastructure (I2I) communications. However, the wireless medium and dynamic nature of these networks expose them to security threats from faulty nodes or malicious attacks. While cryptography-based mechanisms provide security against outsider attacks, the network remains vulnerable to attacks from legitimate but malicious nodes. Trust models have hence been proposed to evaluate node and data credibility to make informed security decisions. Existing models are either vehicle-centric with limited stability due to mobility or infrastructure-based with risks of single points of failure. This paper proposes a self-organizing, infrastructure-based trust model for securing ITS communication leveraging Smart Roadside Signs (SRSs). The model introduces a trust-based clustering algorithm using a fuzzy-based Dempster Shafer Theory (DST). This eliminates dependence on external trusted authorities while enhancing stability through infrastructure oversight. The decentralized trust formation and adaptive clustering balance security assurance with scalability. The results of the simulations show that our model is resilient against on-off attack, packet drop attack, jamming attack, bad-mouthing attack and collusion attack.


## 1 INTRODUCTION


Intelligent Transportation Systems (ITS) are envisioned to enhance traffic management and coordination through the integration of communication technologies into transportation infrastructure. ITS ecosystems comprise interacting vehicles, and roadside infrastructures. Exchanging information through interconnections such as Vehicle-to-Vehicle, Vehicle-to-Infrastructure, and Infrastructure-to-Infrastructure networks. However, the wireless medium and highly dynamic nature of vehicular networks expose them to security threats arising from both malicious attacks as well as inadvertent faults due to physical failure. While cryptography-based security mechanisms can protect against outsider attackers, threats remain from authorized nodes conducting insider attacks and from


faulty nodes transmitting erroneous data.


To address these concerns, trust management models have been proposed for securing ITS networks and to aid real-time decision making on the fidelity of received data and reliability of communication nodes themselves. The majority of existing trust models are vehicle-centric, with nodes evaluating others. However, high mobility of vehicles limited stability in assessment. On the other hand, infrastructure-based trust models rely on fixed nodes such as Road Side Units (RSUs) for trust evaluation and Trusted Authorities for credential and certificates management but remain prone to single point failures. Centralized architectures also pose scalability challenges.

This paper develops a self-organizing infrastructure-supported trust mechanism for reliable ITS networking, called Infrastructure-based Communication Trust model for Intelligent Transportation Systems (ICT4ITS). The model employs Smart Roadside Signs (SRS) as distributed infrastructure entities to facilitate trust formation through collaborative assessment (Abidi et al., 2023). The

<sup>a</sup> <https://orcid.org/0009-0002-5540-7222>

<sup>b</sup> <https://orcid.org/0000-0002-6108-7854>

<sup>c</sup> <https://orcid.org/0000-0002-6953-2086>

<sup>d</sup> <https://orcid.org/0000-0002-9805-6859>

hybrid architecture balances scalability, with stability and ensures the resiliency for security requirements.

In what follows, we define our main contributions: (1) we introduce an infrastructure-based trust model to ensure the stability of the network; (2) propose a self-organizing Manager SRS election and monitoring to enhance the scalability of the network, (3) and employ a fuzzy-based Dempster Shafer Theory technique to evaluate the trustworthiness of the SRSs. The rest of the paper is organized as follows: section 2 briefly reviews the existing trust models. Section 3 introduces the architecture of the model, highlights its overall workflow and defines its considered parameters. The detailed description of the model is presented in section 4. The results are discussed in section 5. Section 6 concludes the paper.

## 2 LITERATURE REVIEW

Securing communications and establishing trust between nodes is essential for the adoption of ITS applications. In what follows, we review the state of the art in order to analyse recent research on trust models and security mechanisms for enabling reliable communication in ITS.

Eunice and Juvanna proposed a secured multi-hop clustering protocol that uses a weighted voting-based cluster head election (Eunice and Juvanna, 2019). Nodes monitor behavior locally to evaluate trust levels. While providing authentication and integrity, the decentralized approach can introduce communication overhead. Kerrache introduced a trust-aware architecture using named data networking to form trusted vehicle groups (Kerrache, 2022). A trusted third party evaluates nodes based on credentials, recommendations and plausibility checks. However, frequent key distribution may lead to scalability issues. Gupta et al. developed an enhanced beacon trust management model integrated with a clustering protocol (Gupta et al., 2023). Malicious nodes are detected using plausibility checks on periodic beacons. The authors use vector points that represent the vehicle's position, speed, and driver direction sent in the beacon message. On the one hand, a centralized server is employed to analyse and compare the messages and detect malicious nodes using predefined thresholds sets. On the other hand, vehicles' densities and velocities change rapidly due to the dynamic nature of VANET. Thus, the centralized threshold-based mechanism lacks adaptability to dynamic topologies. Kchaou et al. presented a secured clustering technique using proxy re-encryption to enable authorized data sharing between cluster members. But the single

cluster head is a single point of failure (Kchaou et al., 2018). Hasrouny et al. used an opinion dynamics-based model for establishing trust relations between nodes to select reliable group leaders (Hasrouny et al., 2019). Alsuhli et al. introduced a double-headed clustering structure to improve resilience to targeted attacks on cluster heads (Alsuhli et al., 2019). The decentralized approach enhances reliability but latency and overhead needs evaluation. Fatemidokht and Rafsanjani proposed a quality of service and monitoring-based clustering algorithm that detects misbehaving nodes (Fatemidokht and Kuchaki Rafsanjani, 2020). The multi-metric decision enables adaptive clustering based on dynamic contexts.

Scalability constitutes a major constraint for the communication trust models. For instance, the authentication schemes proposed in (Eunice and Juvanna, 2019) and (Kerrache, 2022) arise the scalability issue, due to the increase of communication overhead and latency. Moreover, the stability concern occurs, with the lack of awareness of the dynamic nature of the ITS environment, the high speed movement of the vehicles, and by employing centralized architectures that increase the risk of single point failure, such as in (Gupta et al., 2023), and (Kchaou et al., 2018). On the one hand, most recent works deployed decentralized approaches for self-organized trust establishment between vehicles without dependence on external infrastructure. While this method provides better scalability and avoids single points of failure, it lacks the stability of the network. On the other hand, most of the infrastructure based models rely on a single trust authority and they are mainly used for certificate and credential managements, which ensures stability but lacks scalability and increases the risk of a single point failure. Exploring models that introduce a trade-off between the scalability and stability of the network, while ensuring the robustness of the communication, maybe a promising research direction to meet the requirements of ITS applications.

In our proposed model, we combine the infrastructure based model with the self organizing trust, by introducing the Smart Road Signs, where the trust establishment is realized based on cooperation of the SRSs. This combination ensures the scalability and stability of the network while securing the network communication and increasing the robustness of the model.

## 3 SYSTEM DESIGN

This section introduces the architecture of the proposed model, the main phases of the trust workflow,

and the considered attacks and parameters.

### 3.1 ICT4ITS: Architecture

In this paper, we introduce a decentralized communication trust model for ITS leveraging different components including Smart Road Signs (SRSs) and a watchdog module. Figure 1 outlines the overall system architecture.

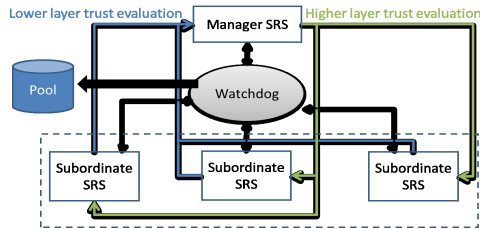


Figure 1: General architecture of the ICT model.

We propose partitioning the traffic road system into regional areas constituting sets of connected roads with embedded regulatory nodes. These oversight nodes, consisting of SRSs, govern traffic data flows within their regional roads. Specifically, SRSs are signs equipped with digital displays that provide real-time traffic notifications to drivers, enabled by processing capabilities and internet connectivity. We configure SRSs in a hierarchical structure with two types: Manager SRSs and Subordinate SRSs, as defined in (Sahli et al., 2022). Managers oversee Subordinates within their supervised region. Furthermore, our framework incorporates watchdog modules as described by Siddiqua et al. (Siddiqua and Jahan, 2022) and Akwirry et al. (Akwirry et al., 2022). The watchdog inclusion constitutes an important element that boosts reliability within our model. These overseer components are deployed within a Trusted Execution Environment (TEE) to securely monitor incoming and outgoing traffic of other entities inside the transmission range. In particular, the watchdog can overhear network activity among nodes as long as they reside within proximity and save them in its pool. By eavesdropping on packet routing of nearby SRSs, the watchdog verifies whether packets are correctly forwarded to the subsequent node. Moreover, according to Akwirry et al. (Akwirry et al., 2022), watchdogs may be leveraged to evaluate transmission trustworthiness levels and perform computational analyzes. Thus, the watchdog's omnidirectional monitoring capability facilitates the calculation of accurate trust values of SRSs within its region.

We propose a two-layer trust evaluation. In the lower layer trust evaluation, Subordinate SRSs use fuzzy logic to estimate the trustworthiness of neigh-

bouring SRSs. The output of the lower layer evaluation of each Subordinate SRS is transmitted to the Manager SRS for aggregation. Accordingly, Manager SRS applies the DST for trust aggregation in the higher level trust evaluation.

### 3.2 ICT4ITS: System Overview

The SRSs are exposed to potential security threats and they may even transmit erroneous information. Since Manager SRSs aggregate the evaluations of the Subordinate SRSs and dictate regional operations, their security impacts the overall system functionality. Accordingly, ensuring trustworthy Manager SRSs constitutes critical network vulnerability. We propose a trust framework centred on SRS behavioural analysis to enhance communications security within SRS nodes. The proposed model enables classification of SRS nodes as either malicious or honest based on observed metrics. The proposed model aims to establish a stable and trusted SRS cluster through two key phases. Firstly, during the election phase, SRSs participate in a competitive election process to select a Manager SRS. Subsequently, in the Manager SRS Observation phase, Subordinate SRSs exchange packets with the Manager to report traffic state information. These packets are then used to continually evaluate cluster components behaviour based on the quality of the communication.

The election relies on an initial trust assessment across SRSs. The SRSs exchange a designated number of packets. The process runs in a bi-directional way to enable mutual evaluations between all SRSs. Then, each SRSs feed Quality of Service indicators (QoS), stored in the pool of the watchdog module, as inputs to its fuzzy inference system to estimate the trustworthiness of neighbouring SRS nodes.

Upon completing the peer trust evaluations via fuzzy logic, the integrated watchdog aggregates the trust level outputs to identify the most trusted SRS to appoint as Manager.

For Manager SRS observation, our hierarchical topology minimizes packet exchange. Subordinate SRSs forward packets to the Manager, similarly to the election process. Concurrently, the watchdog records communications while Subordinates evaluate each other through fuzzy logic, utilizing observed parameters as inference inputs. Subordinates broadcast assessments to the Manager, which aggregates them using Dempster Shafer Theory (DST). The Manager relays the integrated evaluation back to Subordinates.

Subordinate SRSs compare the Manager SRS's trust evaluations against locally computed assessments. If the Manager's assessed trust value for a

monitored node diverges from the Subordinate’s evaluation by an established acceptable threshold range, the Subordinate deems the Manager’s judgment as honest. However, if the Manager’s rating exceeds the permissible differential gap (maximum trust value deviation tolerated), the Subordinate may determine the Manager has acted maliciously or erroneously in an inaccurate manner. Through this comparative analysis, Subordinates can check and balance the Manager’s evaluations based on ground truth local observations. Thereby, the integrity of centralized hierarchical decisions gets enhanced by distributed oversight of lower-level SRSs. Accordingly, if more than 2/3 of the Subordinates estimate that the Manager has acted maliciously, a new election phase is triggered.

### 3.3 ICT4ITS: Attack Model

In this paper, we consider the following communication related attacks (Shetty and Manjaiah, 2022).

- **Packet Drop Attack (PDA).** Malicious node drops a number of packets, intentionally or unintentionally, disrupting communication and leading to packet loss.
- **Jamming Attack (JA).** Malicious nodes inject multiple packets into the network to overcharge it, causing network congestion.
- **Bad-Mouthing Attack (BMA).** Malicious nodes collude to ruin the reputation of well-behaved nodes by providing fake negative feedback, undermining trust and credibility.
- **On-Off Attack (OOA).** Malicious nodes provide random attacks by injecting erroneous data arbitrarily, disrupting communication intermittently.
- **Collision Attack (CA).** Multiple nodes collaborate to harm the network by intentionally performing attacks, interfering with legitimate message transmission and causing data corruption or loss.

### 3.4 ICT4ITS: Considered Parameters

In the proposed model we consider the factors that affect the communication performance between the SRSs. Accordingly, we use packet delivery rate, throughput, end-to-end delay, and error rate as parameters to evaluate the trustworthiness of the SRSs. In what follows, we define these parameters:

- **Packet Delivery Rate (PDR):** Defined as the ratio between effectively received packets versus total packets transmitted. Higher PDR correlates to more reliable delivery, as larger discrepancies in-

dicating potential disruptions degrading availability:

$$PDR = \frac{\text{Total Received Packets}}{\text{Total Sent Packets}} \quad (1)$$

- **Throughput:** Throughput quantifies the amount of data successfully conveyed across the network over a set time window. Higher throughput enables dependent real-time services by promoting responsiveness:

$$\text{Throughput} = \frac{\text{Total Transmitted Packets}}{\text{Total Time}} \quad (2)$$

- **End-to-end delay:** Represents packet travel time from source to recipient. Low latency boosts suitability for time-critical transportation applications sensitive to lag:

$$\text{End-to-end delay} = \frac{\sum(\text{Receive Time} - \text{Send Time})}{\text{Total Received Packets}} \quad (3)$$

**Error Rate:** It measures the proportion of packets lost compared to the total packets transmitted over a specified time period. Lower error rates signal heightened delivery dependability:

$$\text{Error Rate} = \frac{\text{Number of Lost Data Packets}}{\text{Total Sent Packets}} \quad (4)$$

- **Number of packets:** It refers to the number of times a task enters a send sleep state awaiting the transmission of packets to the destination node. In this parameter, we consider that the nodes exhibit a restricted capacity permitting only singular packet broadcasts at discrete times, necessitating interim sleep states between each networked send operation.

The deployed watchdog module is dedicated to passively monitor communications and obtain ground truth recordings of the before-mentioned parameters that are used for trust computation. In fact, the PDR and throughput metrics serve as indicators to detect PDA. The Number of Packets metric aids in identifying OOA. Furthermore, end-to-end delay and error rate metrics are instrumental in detecting JA.

## 4 ICT4ITS: OPERATIONAL PHASE DESCRIPTION

As vehicle networks exhibit inherently dynamic and uncertain environments, fuzzy logic provides VANET-based systems with flexible, adaptive decision-making capabilities by leveraging human expert knowledge. This suitability for handling inexact real-world inputs endows fuzzy architectures with

an apt trust scoring mechanism for SRS components reliant on variable network transmission reliability. Fuzzy logic is composed mainly of three steps defined as follows (Zadeh, 2004): (1) fuzzification, where crisp input values are translated into degrees of membership across fuzzy sets using functions like sigmoid, trapezoidal, Gaussian, or triangular (Pedrycz, 1994); (2) inference system, which involves mapping fuzzified inputs to outputs through if-then rule sets; (3) defuzzification, where fuzzy output sets are quantified into singular or multiple values using methods like centroid, bisector, or mean of maxima (Saade and Diab, 2000).

In our model, we adopt the triangular presentation as fuzzifier due to its simplicity and efficiency (Souissi et al., 2023). We use the inference system proposed in (Umoren et al., 2019). Finally, we apply centroid technique based on its demonstrated effectiveness for consolidating expressions of incomplete knowledge into decisive score reporting (Saade and Diab, 2000). The Subordinate SRSs' fuzzy systems take as an input the packet delivery rate, throughput, number of packets, end-to-end delay, and error rate. In what follows, we present the linguistic variables associated to each input: Packet delivery rate [low, moderate, high], throughput [very low, low, moderate, high], number of packets [less, average, more], end-to-end delay [short, normal, long], and error rate [very low, low]. The linguistic terms associated to the output are: trustworthiness [very low, low, moderate, high]. Figures from 2-6 represent the membership functions of the input variables and figure 7 presents the membership function of the output variable.

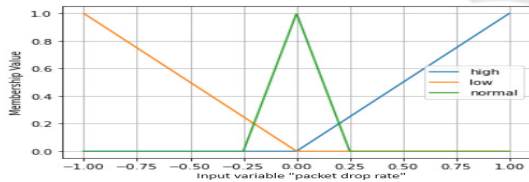


Figure 2: Fuzzy classes and membership functions for the packet delivery rate.

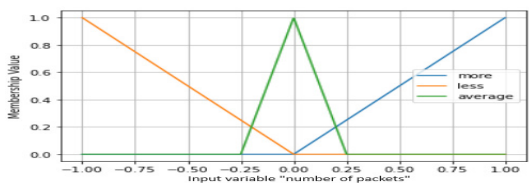


Figure 3: Fuzzy classes and membership functions for the number of packets.

Our model adopts Mamdani fuzzy inference for mapping the input parameters to the trustworthiness of the SRSs using a fuzzy rule-based system (Rahim

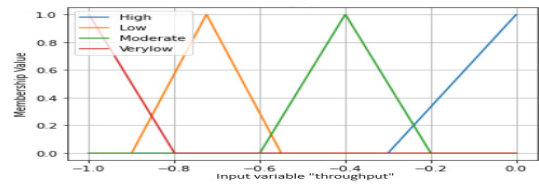


Figure 4: Fuzzy classes and membership functions for the throughput.

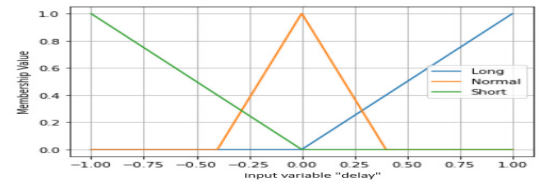


Figure 5: Fuzzy classes and membership functions for the end-to-end delay.

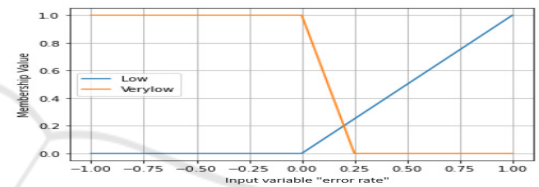


Figure 6: Fuzzy classes and membership functions for the error rate.

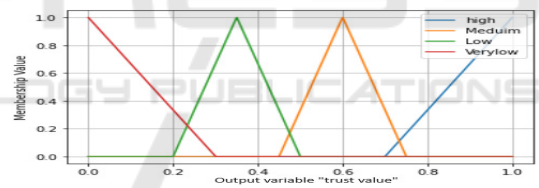


Figure 7: Fuzzy classes and membership functions for the output.

et al., 2017). Our engine utilizes the Mamdani min-max implication approach for discerning rule consequences. We used the rule base proposed in (Umoren et al., 2019). However, this rule base relies primarily on the detection of packet loss and lacks specific representations that characterize jamming attacks. Accordingly, we added the missing rules developed through analysis of analytical data collected from simulated jamming attack scenarios. Table 1 describes the structure of the IF-THEN of the additional clauses. Thereafter, defuzzification phase is executed. We adopt the widespread Centroid method which finds the center of gravity (COG) slice-point equally partitioning the aggregation mass for maximum representativeness, as follows:

$$CoG = \frac{\int_X x \cdot \mu_A(x) dx}{\int_X \mu_A(x) dx} \quad (5)$$

Where  $\mu_A$  is the set of membership functions of the

fuzzy set  $A$  and  $x$  is the variable over the universe of discourse  $X$ .

We employ Dempster-Shafer theory (DST) as an aggregator for consolidating potentially disparate trust evaluations estimated by Subordinate SRSs nodes into a unified assessment. In fact, we leverage DST for modelling uncertain reasoning. As an evidence-based mathematical approach, DST proves useful in decision-making scenarios exhibiting incomplete or conflicting insights. To this end, we convert the fuzzy outputs of the lower layer trust evaluation to belief functions.

Let  $A$  be the output set of a subordinate SRS's fuzzy inference system, where  $A_1, A_2, A_3$ , and  $A_4$  are the elements of the fuzzy output set obtained from a fuzzy inference system, that represents the trustworthiness estimated by one subordinate SRS of one of the neighbouring SRSs. We convert each fuzzy output set  $A_i$  into a belief function  $m_i$  using a mapping function  $f_i$  that assigns Basic Probability Assignments (BPAs) based on the degree of membership of each element in the output set:

$$m_i(x) = f_i(\mu_{A_i}(x)), \quad (6)$$

where  $x$  is an element in the frame of discernment. In this context, the frame of discernment is the set  $A$  that encompasses all possible linguistic terms that the output variable, the trustworthiness, can take.  $A_i$  is the linguistic term of the output of the fuzzy system, with terms [very low, low, moderate, high].  $\mu_{A_i}(x)$  represents the membership function of each term.

Therafter, we combine the belief functions  $m_{11}, m_{21}, m_{31}, m_{41} \dots m_{4n}$ , representing the BPAs of each belief function  $m_i$  of the SRSs, using DST combination's rule as follows:

$$CT = m_{11} \oplus m_{21} \oplus m_{33} \oplus m_{41} \oplus \dots \oplus m_{4n} \quad (7)$$

Where  $CT$  is the current trust value and  $n$  is the number of the SRSs. The fuzzy-based DST provides a pathway for consolidating distributed evaluations under imprecise conditions. Overall, this fuzzy-to-evidential pipeline supports coherent centralized trust evaluation within decentralized ITS environments by combining localized uncertainty management with global consistencies. The aim of this combination is to increase the accuracy of the evaluation and enhance the robustness of the network. After evaluating the current trustworthiness of each SRS using the fuzzy-based DST, we update their trustworthiness using a dynamic weighted sum as shown in Equation 8:

$$Updated\_trust\_value = \alpha \cdot CT + \beta \cdot HT \quad (8)$$

Where  $CT$  is the newly assessed trust value and  $HT$  is the historical trust value.

This consolidates the recent evaluation with historic trustworthiness to balance temporary fluctuations with overall trends. The  $\alpha$  and  $\beta$  parameters determine weighting concreted to new versus old evaluations respectively. We implement an adaptive tuning approach for  $\alpha$  and  $\beta$  assignments to provide custom credibility response rates per SRS based on past performance profiles. Well-behaved nodes are assigned higher  $\alpha$  prioritizing current evaluations to quickly improve standing. However, for SRSs exhibiting bursts of maliciousness, higher  $\beta$  maintains influence of prior windows to dampen volatility effect. Accordingly, if the old trust value of the SRS is higher than 0.6 we assign 0.7 to  $\alpha$  and 0.3 to  $\beta$ . If the old trust value ranges between [0.4, 0.6], we assign a neutral weight to  $\alpha$  and  $\beta$  equals to 0.5. Finally, if the old trust value is lower than 0.4, we prioritize higher  $\beta$  value equals 0.7 and lower  $\alpha$  equals to 0.3. Thereby, misbehaving SRSs require more consistent integrity demonstrations before trust value upgrades. This strategy strengthens resilience against strategic oscillation tactics aimed at briefly feigning good behaviour to swiftly regain network standing after attacks. Through tailored weighting, we promote fair credibility aggregation while preventing exploitation.

## 5 PERFORMANCE EVALUATION

In this section, we present the simulation setup and and discuss the results. In order to generate the data, we used Network Simulator (NS2). NS2 is an open-source, event-driven simulator, designed specifically for research in computer communication networks. Moreover, we used Generator Network Simulator (GNS2) for the script generation, which is a software based on the drag and drop technique to generate the Tool Command Language (TCL) for NS2 of the defined scenario.

Our simulation scenario comprises 10 nodes, representing our SRSs, situated within shared wireless transmission range modeling a decentralized network within the same cluster. The Nodes perform as the data sink and/or active sources. Traffic generation occurs via File Transfer Protocol (FTP) encapsulated through Transmission Control Protocol packet (TCP) for reliability. We configure TCP agents on each node to handle connection setup, data transfer, flow control and event handling. FTP is a protocol used for transferring files between computers on a network. It is not characterized by a constant bit rate, but rather involves the transfer of files, which may vary in size and number, and may take varying amounts of time to transmit. During simulation execution, we gather

Table 1: Rules base structure.

Packet delivery	Throughput	Number of packets	Delay	Error rate	Trust
high	high	Average	long	low	low
high	high	more	long	low	low
high	high	Average	normal	low	low
high	high	more	normal	low	low
high	very low	Average	long	low	low
high	very low	more	long	low	low
high	very low	Average	normal	low	low
high	very low	more	normal	low	very low
high	high	Average	long	low	low
high	high	more	long	low	very low
high	high	Average	normal	low	low
high	high	more	normal	low	low
high	very low	Average	long	low	low
high	very low	more	long	low	very low
high	very low	Average	short	very low	high
high	very low	Average	normal	low	medium
high	very low	more	normal	low	very low
high	high	Average	long	low	low
moderate	high	more	long	low	very low
moderate	high	Average	normal	low	low
moderate	high	more	normal	low	very low
moderate	very low	Average	long	low	low
moderate	very low	more	long	low	very low
moderate	very low	Average	normal	low	low
moderate	very low	more	normal	low	low
moderate	high	Average	long	low	low
moderate	high	more	long	low	low
moderate	high	more	normal	low	low
moderate	high	Average	normal	low	low

per-flow metrics including delay, error rate, delivery rate, throughput and absolute packet deliveries.

In what follows, we discuss the numerical results of the trust model across different scenarios to assess its robustness in the presence of different attacks and the stability of the cluster formation. In all subsequent figures, the x-axis denotes the number of iterations, while the y-axis represents the trust value of the SRSs.

### 5.1 Model's Robustness Evaluation

In order to evaluate the robustness of our model, we examine its performance in the presence of different percentages of malicious nodes and various attacks.

In the first scenario, we test the resiliency of our model against on-off attack and packet drop attack. Accordingly, we track the evolution of the trust value of a well-behaving node and a malicious node performing packet drop attack within on-off mode. The results of the experimentation are presented in figure 8. The malicious SRS performed the PDR in the following iterations: 2, 4-9, 13-15, 18-20, 24, 27-29.

In the second scenario, we test the resiliency of the proposed model against on-off attack and bad mouthing attack, as presented in figure 9. In this sce-

nario, the malicious SRS performed attacks at iterations number: 1-5, 11-5, 22-25.

In both scenarios, the malicious SRS and the benign SRS have initial trust value equals to 0.5. We notice in figure 8 and 9, that the trust value of the malicious node decreases rapidly whenever it starts performing the malicious attacks. However, when it readopts a good behaviour, the trust value is slowly growing compared to the drop rate when it performs attacks. This is due to the adaptive weight of the trust update. In fact, when the malicious nodes presents a good behaviour after being malicious the model uses higher  $\beta$  value. Accordingly, the trust updates rely more on old trust evaluation, which requires the malicious node to present a good performance for a long time window to upgrade its trust value. This mechanism allows our model to track alternative behaviour of malicious nodes and detect their attacks.

In the third scenario, we test the robustness of our model against packet drop attack, jamming attack, and bad mouthing attack, as shown in 10, 11, and 12, respectively. Unlike the first and second scenario, in this scenario the malicious SRS are constantly performing attacks. As shown in the figures, the benign SRSs quickly converge to a high trust value. Simi-

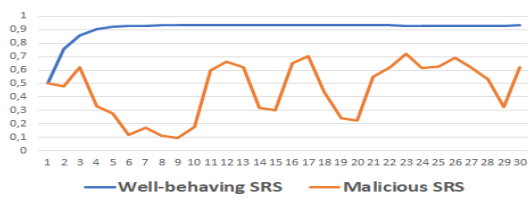


Figure 8: Trustworthiness of a well-behaving SRS and a malicious SRS performing OOA and PDA.

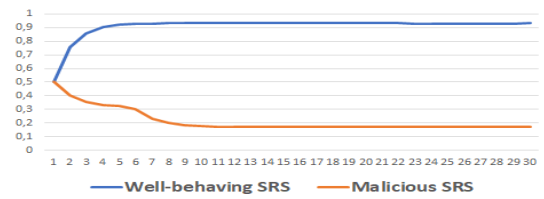


Figure 12: Trustworthiness of a well-behaving SRS and a malicious SRS performing BMA.

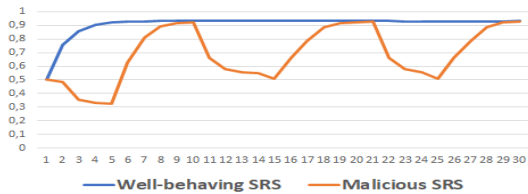


Figure 9: Trustworthiness of a well-behaving SRS and a malicious SRS performing OOA and BMA.

larly, the malicious SRSs converge rapidly to a low trust value after few iterations of performing attacks. This can be explained by the employment of a fuzzy-based DST for trust computation. This mechanism allows the model to increase the accuracy of the evaluation by handling the uncertainty of the data. The two-layer evaluation enhance the visibility of the environment by combining more evidence to ensure the accuracy of the evaluation and the robustness of the network. Moreover, the adaptive trust update mechanism ensures that the update of the trust values of benign SRS consider recent trust evaluation for rapid growth. On the other hand, it ensures that the trust update for the malicious SRSs considers more old trust values, guaranteeing a quick decrease of their trust value among the iterations.

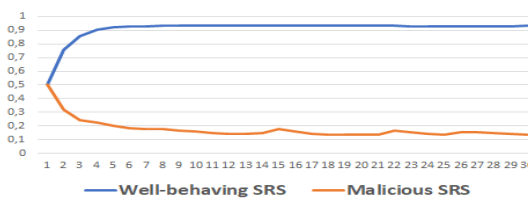


Figure 10: Trustworthiness of a well-behaving SRS and a malicious SRS performing PDR.

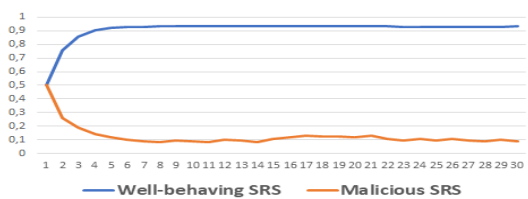


Figure 11: Trustworthiness of a well-behaving SRS and a malicious SRS performing jamming attack.

## 5.2 Cluster Stability Evaluation

In the last experimentation, we examine the stability of the cluster by examining the time laps before starting a new Manager election phase. Moreover, we examine the trustworthiness of the Manager in the meantime. In this scenario, we suppose that the Manager is well-behaving and in the first 15 iterations, we inject 1/3 of the number of the Subordinate SRSs performing BMA. After iteration 15, we increase the percentage of the malicious nodes to 2/3 out of the total subordinate SRSs. The results of the experimentation are plotted in figures 13, and 14, respectively. The figures show that whenever the number of the malicious nodes performing BMA is less than the 2/3 of the Subordinate SRSs, the fake feedbacks do not affect the stability of the cluster and the trustworthiness of the Manager. However, after iteration 15 the trustworthiness of the Manager decreases, although its is a benign SRS and a new election process is triggered. This can be explained by the fact that when the number of the malicious SRSs performing BMA increases, the combination of their evaluations affects the final evaluation. However, it is worth mentioning that this case scenario is unrealistic and it is implausible to have more than 2/3 of the SRS to become compromised simultaneously.

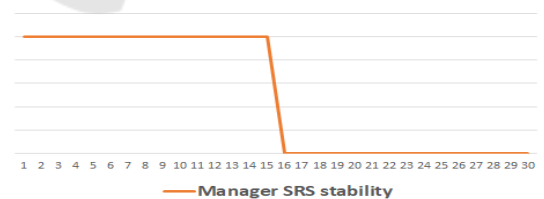


Figure 13: Stability of the Manager SRS.

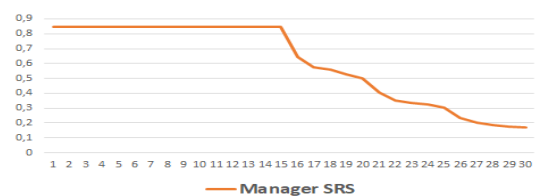


Figure 14: Trustworthiness of the Manager SRS.



## 6 CONCLUSIONS

The paper introduces a decentralized trust management model for electing trustworthy Manager SRS and forming stable clusters. It ensures continuous cluster monitoring by tracking Manager SRS behavior via collaborative assessment among subordinate SRSs. The proposed model integrates the stability of infrastructure-based evaluation with the scalability and resilience of decentralized trust architecture. Self-organizing clustering dynamically selects trusted Managers, reducing communication overhead and eliminating single point failures. Trust computation, using fuzzy logic and DST, increases the accuracy of trust evaluation by handling the uncertainty of the input and the conflicted outputs of the SRSs. Simulation-based evaluation reveals resilience against OOA, PDA, JA, BMA, and CA but struggles with collusion and BMA when malicious SRSs exceed 2/3 of the total. Despite potential computational complexity, combining fuzzy inference with DST strengthens the network, offering robustness and flexibility for uncertain and conflicting evidence. Future work includes evaluating response time and incorporating social metrics like honesty and cooperativeness to enhance trust evaluation accuracy.

## ACKNOWLEDGEMENTS

The research leading to these results has received funding from the Ministry of Higher Education, Research and Innovation of the Sultanate of Oman under the Block Funding Program. Block Funding Agreement No [BFP/RGP/ICT/22/327].

The English quality of the paper is enhanced using the AI assistant Claude (Anthropic, 2023).

## REFERENCES

- Abidi, R., Sahli, N., Trojet, W., Azzouna, N. B., and Hoblos, G. (2023). An infrastructure-based trust management framework for cooperative ITS. In *VEHITS*, pages 329–336.
- Akwirry, B., Bessis, N., Malik, H., and McHale, S. (2022). A multi-tier trust-based security mechanism for vehicular ad-hoc network communications. *Sensors*, 22(21):8285.
- Alsuhli, G. H., Khattab, A., Fahmy, Y. A., et al. (2019). Double-head clustering for resilient vanets. *Wireless communications and mobile computing*, 2019.
- Anthropic (2023). Claude - AI assistant. <https://www.anthropic.com/claude>. [Online; accessed 23-February-2023].
- Eunice, K. S. and Juvanna, I. (2019). Secured multi-hop clustering protocol for location-based routing in vanets. *International Journal of Advanced Computer Science and Applications*, 10(4).
- Fatemidokht, H. and Kuchaki Rafsanjani, M. (2020). Qmmvanet: An efficient clustering algorithm based on qos and monitoring of malicious vehicles in vehicular ad hoc networks. *Journal of Systems and Software*, 165:110561.
- Gupta, C., Singh, L., and Tiwari, R. (2023). Malicious node detection in vehicular ad-hoc network (vanet) using enhanced beacon trust management with clustering protocol (ebtm-cp). *Wireless Personal Communications*, 130(1):321–346.
- Hasrouny, H., Samhat, A. E., Bassil, C., and Laouiti, A. (2019). Trust model for secure group leader-based communications in vanet. *Wireless Networks*, 25:4639–4661.
- Kchaou, A., Abassi, R., and El Fatmi, S. G. (2018). Towards a secured clustering mechanism for messages exchange in vanet. In *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pages 88–93.
- Kerrache, C. A. (2022). A trust-aware cluster-based communication architecture for vehicular named data networking. *ITU J. on Future and Evolving Technologies*.
- Pedrycz, W. (1994). Why triangular membership functions? *Fuzzy Sets and Systems*, 64(1):21–30.
- Rahim, R. et al. (2017). Comparative analysis of membership function on mamdani fuzzy inference system for decision making. In *Journal of Physics: Conference Series*, volume 930, page 012029. IOP Publishing.
- Saade, J. and Diab, H. (2000). Defuzzification techniques for fuzzy controllers. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 30(1):223–229.
- 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.
- Shetty, S. R. and Manjaiah, D. H. (2022). A comprehensive study of security attack on vanet. In Sharma, N., Chakrabarti, A., Balas, V. E., and Bruckstein, A. M., editors, *Data Management, Analytics and Innovation*, pages 407–428, Singapore. Springer Singapore.
- Siddiqua, F. and Jahan, M. (2022). A trust-based malicious rsu detection mechanism in edge-enabled vehicular ad hoc networks. *arXiv preprint arXiv:2208.05680*.
- Souissi, I., Abidi, R., Azzouna, N. B., Berradia, T., and Said, L. B. (2023). Ecotrust: A novel model for energy consumption trust assurance in electric vehicular networks. *Ad Hoc Networks*, 149:103246.
- Umoren, I. J., Asuquo, D. E., Gilean, O., and Esang, M. (2019). Performability of retransmission of loss packets in wireless sensor networks. *Comput. Inf. Sci.*, 12(2):71–86.
- Zadeh, L. A. (2004). A note on web intelligence, world knowledge and fuzzy logic. *Data & Knowledge Engineering*, 50(3):291–304. Special jubilee issue: DKE 50.