

# Dynamic Trust Modeling In Siov: A Hybrid Multilayer Framework Of Fuzzy Logic, Temporal Dynamics, And Shapley-Based Cooperative Game Theory Under Adversarial Conditions

Alireza Seddighi<sup>1</sup>, Seyyed Amir Asghari<sup>2\*</sup>, Morteza Romoozi<sup>3</sup>, Hamideh Babaei<sup>4</sup>

<sup>1</sup>PhD Student in Computer Engineering, Software System, Department of Computer Engineering, Qom Branch, Islamic Azad University, Qom, Iran

<sup>2</sup>Corresponding Author, Associate Professor, Data Science and Technology Department, University of Tehran, Tehran, Iran

<sup>3</sup>Assistant Professor, Department of Computer Engineering, Kashan Branch, Islamic Azad University, Kashan, Iran

<sup>4</sup>Assistant Professor, Department of Computer Engineering, Naragh Branch, Islamic Azad University, Naragh, Iran

\*Corresponding Author

## ABSTRACT

In the complex and dynamic environment of the "Social Internet of Vehicles" (SIOV), recognized as a transformative advancement within the Internet of Things domain focusing on human-machine interactions, the concept of trust emerges as a multidimensional, context-dependent, and behaviorally sensitive variable. It plays a fundamental role in ensuring communication security, facilitating intelligent cooperation, and enhancing decision-making processes. This research presents the design and evaluation of a multilayer framework for modeling trust within the intricate and evolving ecosystem of the Social Internet of Vehicles (SIOV). The proposed framework integrates fuzzy logic, fuzzy temporal value analysis, and cooperative game theory to examine trust's behavioral dimensions—honesty, sincerity, privacy, and connectivity—through dynamic temporal modeling and strategic analysis of agent interactions. Leveraging fuzzy approximate inference and simulation within the Veins platform, the model achieved trust estimation accuracy exceeding 89% and identified the IC strategy as the most stable behavioral pattern. Additionally, risk and utility analyses improved decision-making accuracy. Comparative assessments with baseline models demonstrated the proposed framework's performance improvement of 5 to 11 percent. By offering a coherent and generalizable approach, this study significantly contributes to advancing intelligent social systems within the SIOV environment.

**Keywords:** Trust Modeling, Fuzzy Logic, Shapley Value, FNPV, SIOV, Cooperative Game Theory, Strategy Ranking, Vehicular Social Networks, OMNeT++, SUMO, Veins.

## 1- Introduction

In recent decades, smart networks and distributed systems have expanded significantly, transforming numerous critical infrastructures such as transportation, energy, healthcare, and communications [1]. One of the most advanced examples of this transformation is the emergence of Social Internet of Vehicles (SIOV) networks, which integrate the Internet of Things, vehicle-based communication networks, and human-centric social interactions[2][3]. In these networks, vehicles autonomously interact with one another and make real-time decisions that can have vital implications for safety, efficiency, and security [4][5].

Within this context, trust is not optional but a fundamental necessity for the survival and proper functioning of the system. In the absence of classical centralized authentication and validation mechanisms, trust-based decision-making regarding other agents' actions plays a key role in ensuring security and cooperation. Trust, as a cognitive and social mechanism, enables rational decision-making under conditions of incomplete or conflicting information [6]. However, modeling trust in SIOV faces unprecedented challenges: instantaneous interactions, data

volatility, rapid behavioral variability, environmental uncertainty, and structural heterogeneity are just some of the barriers that distinguish trust analysis in this domain from others. Consequently, the development of a precise, adaptable, and reliable framework for trust modeling and decision-making in SIOV is an urgent and critical necessity [7].

### **1-1- Challenges of Trust Computation in Dynamic Environments**

In the domain of Social Internet of Vehicles (SIOV) networks, interactions among agents occur instantaneously within highly variable and dynamic conditions. Unlike traditional systems characterized by stable and predictable communications, agents such as vehicles, nodes, sensors, and infrastructures are mobile, heterogeneous, and often unknown. Communications between nodes are affected by network delays, route fluctuations, and packet loss rates, while agent behaviors may depend on location, time, and memory of prior interactions [8][9]. In such an environment, trust computation as the foundation for decision-making becomes a complex process that must account for continuous environmental changes and enable real-time decisions regarding which agent to trust, at what risk level, and over what time frame. Therefore, the trust model in SIOV must possess memory, predictive capability, adaptability, and interpretability—requirements that exceed the capacity of traditional models and necessitate the design of a multidimensional and dynamic computational model [10][11].

### **1-2- Limitations of Traditional Models (Crisp / Probabilistic / Static Fuzzy)**

The classical literature on trust primarily focuses on three main approaches:

First, Crisp Models assign a numerical score between 0 and 1 to each agent based on fixed rules, usually relying on the success of past interactions. These models disregard environmental variability, lack the capacity to interpret incomplete or uncertain data, and often make decisions in a binary “all-or-nothing” manner [12][13].

Second, Probabilistic Models employ statistical methods such as Bayesian networks or Markov chains to predict the future behavior of agents. However, they assume independence of interactions, fail to capture behavioral or social factors, and perform poorly in environments with limited or incomplete data. Third, static fuzzy trust models, which use fuzzy logic to represent subjective ambiguities such as “high trust” and partially handle linguistic and incomplete data, lack temporal analysis, dynamic mechanisms for trust updating, and the ability to assess multilateral interactions; therefore, none of these approaches can adequately address the complexities, variability, and multidimensionality of trust issues in the Social Internet of Vehicles (SIOV) [14][15].

### **1-3- Weakness in the simultaneous analysis of behavioral, temporal, and strategic factors**

The issue of trust in SIOV (Social Internet of Vehicles) is multidimensional and, based on social and cognitive studies, arises from the interaction of three main groups of factors: First, behavioral factors such as honesty, sincerity or prior familiarity, the degree of privacy adherence, and the quality of communications, which lay the groundwork for understanding the social performance of agents [16][17]; second, temporal factors indicating that trust evolves over time and an agent’s behavior may change or improve through positive interactions, thus the trust model must operate dynamically and cumulatively; and third, strategic factors in multi-agent networks, where agents make decisions based on predicting others’ reactions, the extent of participation in coalitions, and a cost-benefit analysis of cooperative or opportunistic behavior [18][19]. To analyze these, tools such as game theory and collective participation analysis are required. Models that consider only one of these three dimensions do not provide a complete and accurate analysis of trust, and only by combining these layers simultaneously can a realistic, predictable, and reliable understanding of the trust structure in SIOV be achieved [20][21].

### **1-4- The Need for a Multilayered Framework Supporting Adaptation and Explanation**

Given the existing challenges and deficiencies, this study emphasizes the necessity of designing a new multilayered framework capable of hierarchically and measurably modeling behavioral factors, accounting for temporal changes through cumulative time-based models such as fuzzy net present value (FNPV), and analyzing the contribution of strategies in strengthening or weakening collective trust using cooperative game theory and fuzzy Shapley value [22][23]. This framework must simultaneously manage environmental dynamics, data uncertainty, and the complexity of agent relationships. Its final model should be numerically precise, conceptually explicable, and operationally implementable, enabling decision-makers to trust it and base their decisions confidently upon it. The present thesis introduces a four-layer framework comprising objectives, IHPC dimensions, FNPV time analysis, and Shapley participation analysis, aiming to provide a comprehensive, scientific, and practical response to

this need. Ultimately, this research seeks to answer how a composite multilayered framework—built on fuzzy logic, temporal value analysis, and cooperative game theory—can model trust among SIOV network agents in a manner that is behaviorally adaptive, interpretable, and feasible for real-world implementation [24][25][26].

## 2- Conceptual Framework of the Research

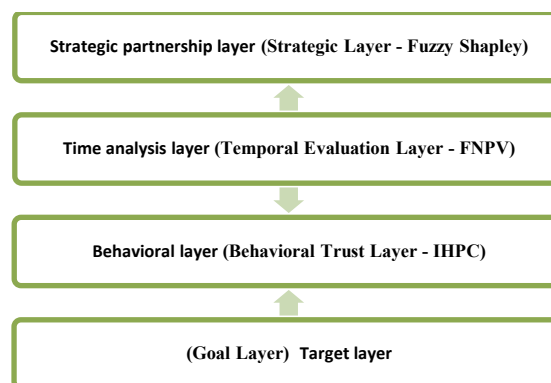
Modeling trust in dynamic, multi-agent, and distributed environments such as Social Internet of Vehicles (SIOV) necessitates a structure capable of simultaneously encompassing the behavioral, temporal, and strategic dimensions of trust while maintaining analytical coherence. This study, relying on a four-layered framework, endeavors to design the process of trust evaluation and analysis in a step-by-step, explicable, and executable manner within operational settings. This conceptual framework is not only theoretically robust but also practical for implementation in both simulation platforms and real-world systems. The subsequent sections provide a detailed exposition of its various dimensions.

### 2-1- Layers of the Research Conceptual Framework

The research conceptual framework is designed as a four-layered structure, where each layer plays a specific role in the analysis, evaluation, and production of the final trust outcome. These layers, in order, are as follows:

1. Goal Layer: Defines the overarching objective of trust-building within the network (e.g., increasing average trust, reducing behavioral deviations, optimizing partner selection)
2. Behavioral Trust Layer (IHPC): Analyzes four key behavioral dimensions—Honesty (H), Intimacy (I), Privacy (P), and Communication (C)—using fuzzy logic
3. Temporal Evaluation Layer (FNPV): Assesses the trend of trust variations over behavioral episodes by applying a discount rate
4. Strategic Collaborative Layer (Fuzzy Shapley): Examines coalitions, ranks strategies, and allocates the contribution of each agent in strengthening or weakening collective trust.

Figure 1-1 illustrates the four hierarchical levels of the research conceptual framework, beginning with the high-level goal setting and proceeding sequentially through behavioral trust analysis (IHPC), temporal evaluation of trust dynamics (FNPV), and strategic coalition analysis based on fuzzy Shapley value.



**Figure 1** Layers of the research conceptual framework

### 2-2- The Role of Each Layer in the Final Analysis

Layer 1: Objective (Trust Objective)

This layer is responsible for determining the direction of the analysis. In this study, trust-building objectives may include:

- Maximizing the cumulative level of network trust
- Identifying and removing non-cooperative agents
- Optimizing partner selection in subsequent interactions.

All subsequent analyses are guided by this objective, and the structure of the final output will be a function of it (for example, weighting of dimensions or discount rates may vary according to the objective).

Layer 2: Behavioral Dimension Analysis (IHPC)

This layer models trust from a psycho-social perspective. Each of the four IHPC dimensions is defined fuzzily:

- H (Honesty): Consistent, truthful behavior, free from contradictions or deceit in interactions
- I (Intimacy): Successful prior interactions, prior acquaintance, or behavioral loyalty
- P (Privacy): Respecting data privacy, avoiding excessive data transmission or requests

- C (Communication): Response time, packet loss rate, message coherence

Each of these indicators is converted into base trust through fuzzy membership degrees, which serves as the input for the next stage.

Layer 3: Fuzzy Temporal Analysis (FNPV)

In this layer, the base trust derived from IHPC is transformed into a cumulative behavioral flow over episodes. This analysis is carried out using the following formula:

$$T_{FNPV} = \sum_{t=0}^n \frac{C_t}{(\beta + 1)^t}$$

Where  $C_t$  fuzzy trust in the episode  $t$ ,  $\beta$ , behavioral-temporal discount rate, and  $n$  number of temporal episodes are involved.

Layer 4: Analysis of Participation and Coalitions (Fuzzy Shapley)

In this stage, using the fuzzy Shapley value, the contribution of each behavioral strategy or coalition combination to the formation of the final trust is analyzed. This layer answers the following questions:

- Which strategies, in which combinations, have the greatest positive or negative impact?
- Do some agents, despite poor performance, have reinforcing roles in coalitions?
- Which behaviors should be strengthened or eliminated to maintain trust stability?

The output of this layer can be presented as:

- Ranking of strategies
- Suggestions for stable combinations
- Or identification of divergent behaviors

### 2-3- Relationship between Trust Dimensions and Model Output

Within the framework of the proposed model in this research, trust is analyzed as a multidimensional variable at three main levels:

- At the agent level (analysis of individual trust dimensions based on the IHPC model),
- At the interaction level (temporal behavior analysis and trust dynamics using fuzzy logic and the fuzzy net present value model, FNPV), and
- At the network level (coalitional evaluation using cooperative games and the fuzzy Shapley value).

According to Table 1-1, each of the aforementioned levels possesses its own specific inputs and outputs. At the agent level, trust indicators such as honesty, sincerity, privacy preservation, and communications (within the IHPC matrix framework) function as inputs and result in the generation of a base trust score for each agent. This initial score serves as the foundation for subsequent decision-making processes.

At the interaction level, the dynamics of trust are analyzed with a temporal approach. Here, long-term behavioral trends or oscillatory patterns in agent relationships are identified, and the fuzzy net present value model (FNPV) is employed to calculate cumulative trust levels over defined time intervals.

Finally, the network level is dedicated to analyzing coalition outcomes; utilizing collaborative strategies, the influence power of each agent on the success of various coalitions is assessed, and the model's final output (such as trust intensity, orientation, or persistence) is formed accordingly.

This three-layer hierarchy enables a more precise, dynamic, and interpretable evaluation of trust within distributed and heterogeneous environments such as the Social Internet of Vehicles (SIoV).

The connection between trust dimensions (at the agent level), temporal analysis (at the interaction level), and coalition evaluation (at the network level) is defined within the framework of this research as follows:

**Table 1: Matching the Input Dimensions of Trust with Analytical and Final Outputs in the Proposed Model**

Level of Analysis	Inputs	Intermediate Output	Effect on Final Output
Agent	IHPC (H, I, P, C)	Base trust score	Initial intensity and direction of trust
Interaction / Time	Behavioral episodes	Temporal dynamics analysis of trust (FNPV)	Identification of stable or oscillatory trends in trust formation
Network / Group	Collaborative strategies	Fair share in trust (Fuzzy Shapley)	Evaluation of equity in participation and prioritization of effective strategies

The combination of these three layers forms the final output of the model:

$$T_{final} = f(IHPC, FNPV, Shapley)$$

Wherein it serves as a composite trust metric, forming the basis for decision-making in:

- Validating received messages
- Selecting trusted partners
- Identifying uncooperative behaviors or interactive threats
- Adjusting the level of agent interaction and response based on the trust risk level

The conceptual framework of this research, designed as a four-layered structure, successfully models and analyzes trust integrally from three dimensions: psychological, temporal, and participatory. This framework is not only interpretable, modular, and flexible but also capable of implementation in real-world environments. It can serve as a foundation for developing intelligent, trust-aware systems within the Social Internet of Vehicles (SIoV) domain and beyond.

### 3- Research Methodology

Considering the complexity and uncertainty inherent in social vehicle networks (SIoV), the present study proposes a hybrid approach based on fuzzy logic and game theory. Fuzzy logic is employed to model trust, which is a relative and uncertain concept, enabling more precise analysis across the various spectra of trust. Game theory is utilized to analyze strategic decision-making and interactions among vehicles, particularly within the frameworks of cooperative games and the Shapley value. The integration of these two approaches is designed such that fuzzy logic assesses uncertain trustworthiness, and its outputs serve as inputs to game theory models for analyzing strategies and each agent's contribution. This methodology is scientifically sound and practically implementable and extensible, facilitating a more precise analysis of behaviors in real SIoV environments.

#### 3-1- Rationale for Selection and Scientific Justification of the Chosen Method

The selection of a hybrid approach combining fuzzy logic and game theory in this research is grounded in the specific demands of the problem under investigation and is made in consideration of the limitations and deficiencies of prevalent methods in trust modeling. Trust modeling in Social Internet of Vehicles (SIoV) networks requires a multidimensional and adaptable approach due to characteristics such as dynamic interactions, interdependencies, data uncertainty, and the absence of a centralized decision-making authority. This conceptual and implemented integration establishes a distinctive foundation for analyzing trust in distributed multi-agent environments, an aspect not comprehensively addressed in any recent reference models.

- Limitations of traditional methods
- Capabilities of fuzzy logic in trust modeling
- Role of game theory in analyzing strategic interactions
- The synergistic power of combining both approaches (fuzzy logic + game theory)
- Applicability in real-world environments

#### 3-2- Implementation Steps of the Proposed Framework

The proposed framework encompasses a series of sequential and interactive stages, beginning with the identification of fundamental trust factors and extending to the final ranking of strategies and dynamic updates based on environmental changes. This framework is designed to be conceptually clear and structured, as well as computationally feasible for implementation in realistic simulation environments such as OMNeT++, Veins, and SUMO. The following sections elaborate on the key steps in executing this framework.

- Defining and Quantifying Trust Factors: Identification of four primary trust factors (honesty, intimacy, privacy, communication) and modeling them using fuzzy membership functions.
- Forming the Strategy Matrix: Generating various combinations of strategies based on the levels of trust factors and constructing a multidimensional matrix of possible states.
- Calculating the Fuzzy Net Present Value (FNPV): For each strategy, computing a fuzzy score as an aggregated measure of trust.
- Analyzing Strategy Interactions and Constructing the Utility Matrix: Evaluating the utility of each strategy combination and preparing a matrix for application in game theory.
- Determining Coalitions and Calculating the Fuzzy Shapley Value: By calculating the fuzzy Shapley value for each combination, the contribution of each strategy to the final trust is identified and quantified.
- Ranking and Selecting Optimal Strategies: Strategies with higher Shapley values and lower risk are introduced as preferred options.

- Adaptive Updating and Feedback: The framework is cyclically and adaptively updated in response to environmental changes and feedback, ensuring the model remains efficient and consistent.
- Ultimately, the aforementioned steps provide a transparent, flexible, and implementable framework that facilitates the evaluation and optimal selection of behavioral-trust strategies in complex and dynamic environments.

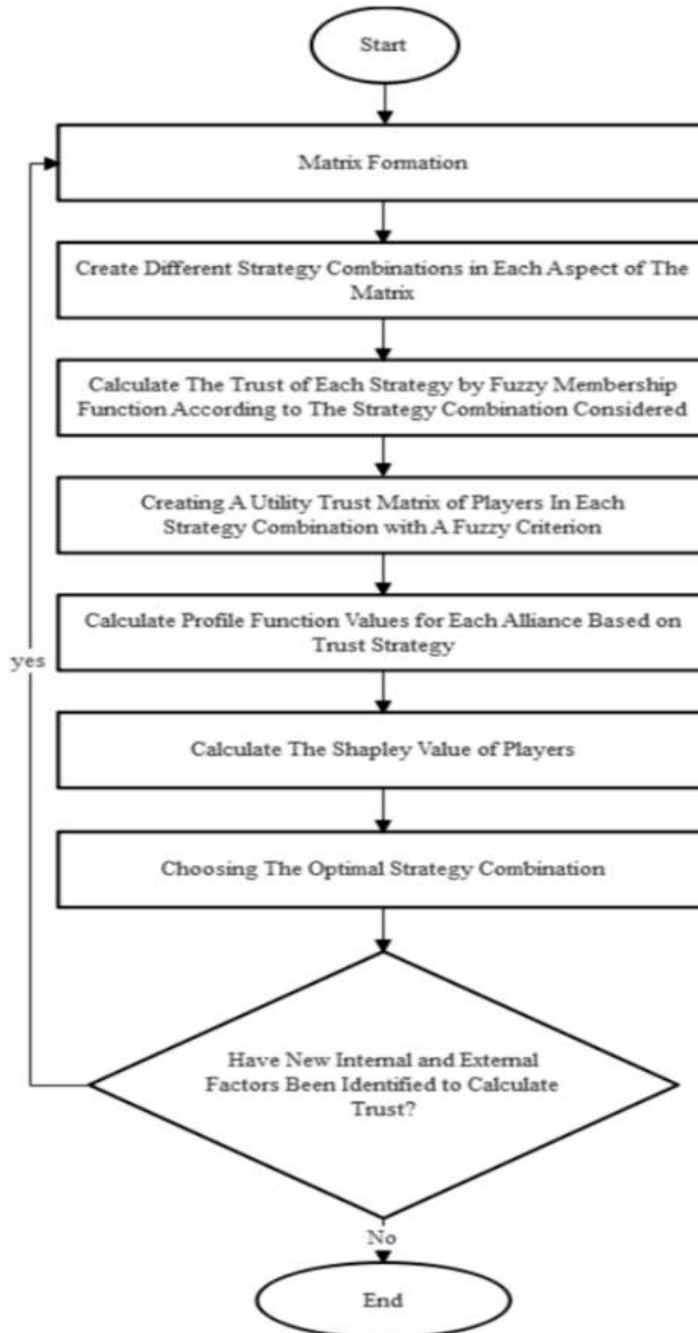


Figure 2 Flowchart of the steps for implementing the proposed framework

### 3-3- Mathematical and Fuzzy Modeling

#### 3-3-1- Net Present Value (NPV)

In the economic analysis of projects and decision-making under conditions involving time-dependent cash flows, one of the critical indicators is the Net Present Value (NPV). This metric calculates the profitability or return of a project by considering initial costs and benefits accrued over time, applying a discount factor.

$$NPV = C_0 + \sum_{t=1}^{\infty} \beta_t \cdot C_t$$

$$\beta_t = \frac{1}{(1+r)^t}$$

where: is  $C_0$  the initial cost (in this model, the degree of negative initial trust or the risk at the start of interaction),  $C_t$  is the benefit flow (in this model, the trust values obtained from interactions at time ),  $\beta$  is the discount factor used to calculate the present value of future benefits, and  $t$  is the number of time steps in the simulation.

### 3-3-2- Fuzzy Net Present Value (FNPV)

Considering that in the real world, trust values are not definitive but rather linguistic, ambiguous, and uncertain, the classical NPV model is insufficient. Therefore, in this study, a fuzzified version of the net present value, named FNPV, has been developed. The general formula of the model is defined as follows:

$$NPV = C_0 + \sum_{t=1}^n \beta_t \cdot C_t$$

where is the  $C_0$  initial cost of the strategy (for example, the baseline trust level or prior belief),  $C_t$  is the benefit derived from the strategy  $t$  at time (such as interaction success rate, network feedback, or improvement in environmental trust),  $\beta_t$  is the behavioral-temporal discount factor within the interval, corresponding to the stability of the relationship, interaction quality, or trust change rate,  $C_0$ , and  $C_t$  are fuzzy numbers (triangular or trapezoidal).

### 3-3-3- Calculating the Utility of Strategies

After computing the Fuzzy Net Present Value (FNPV) for each strategy, the objective is to extract the fuzzy utility of each strategy to enable its application in decision analysis and game theory; here, (a, b, c) represent the three vertices of the final fuzzy membership function of the FNPV.

$$Utility = \frac{a+b+c}{3}$$

### 3-3-4- Generalized Fuzzy Formulation for Ranking Strategies and Calculating Utility

In this section, a generalized framework is presented for ranking fuzzy behavioral strategies, designed to integrate two key criteria: average utility and minimal risk. This approach allows us to consider not only the overall value of a strategy (its mean) but also the impact of potential negative outcomes on the final decision-making process. For each strategy  $i$ , the final output is defined as a triangular fuzzy number:

$$T_i = (a_i, b_i, c_i)$$

where the lower bound of the fuzzy value represents the minimum confidence or maximum risk, the peak membership value indicates a high-confidence point, and the upper bound sets the highest fuzzy value.

## 3-4- Modeling Using Game Theory

Trust analysis in complex networks such as the Social Internet of Vehicles (SIOV) cannot be accomplished solely by considering individual criteria, since the behavior of each agent is influenced by the strategies of other agents. Under these conditions, the use of cooperative game theory provides an effective approach to examine collective interactions and assess the relative contribution of each agent toward enhancing the overall trust level.

### 3-4-1- Cooperative Games

Cooperative games are a category within game theory models where agents can form coalitions and collaboratively work as a group to enhance their collective payoff. In the proposed model, agents participate in trust coalitions by combining their strategies. The objective is to assess the extent to which each agent or strategy contributes to the establishment of stable and beneficial trust. Since this contribution depends on interactions with other strategies, it is modeled using cooperative game theory.

### 3-4-2- Shapley Value

The Shapley value is a fundamental tool in cooperative game theory used to fairly allocate each player's

share of the total coalition payoff. Introduced by Lloyd Shapley, this concept is based on analyzing all possible sequences in which players may join the coalition and calculating each player's final share accordingly. For a set of players ( $N$ ) and a coalition value function representing  $v(S)$  the payoff of coalition  $S \subseteq N$ , the share of player is computed as follows:

$$\phi_i(v) = \sum_{S \subseteq N \setminus \{i\}} \frac{|S|!(|N| - |S| - 1)!}{|N|!} [v(S \cup \{i\}) - v(S)]$$

Where  $\phi_i$  denotes the Shapley value for player,  $i$ ,  $S$  is a subset of players excluding,  $i$ ,  $|S|$  is the size or number of members in coalition,  $v(S \cup \{i\}) - v(S)$ ,  $v(S)$  is the total value of coalition,  $v(S)$  is the marginal contribution of player  $i$  to the coalition,  $S$  represents all coalitions that  $S \subseteq N \setminus \{i\}$ , do not include player,  $N$  is the set of all players (available strategies).

### 3-4-3- Fuzzy Shapley Value

In situations where the values of coalitions are defined fuzzily or imprecisely, as in the current trust model where outputs are calculated in a fuzzy manner (FNPV), the classical Shapley value is insufficient. In such cases, the fuzzy Shapley value must be employed. The rationale for this stems from the fact that the output values of each strategy are fuzzy (triangular or trapezoidal), the benefits of coalition participation are not merely numerical but involve an uncertainty range, and the model requires an accurate assessment of the impact of participation within an uncertain environment.

## 3-5- Simulation and Implementation of the Model

### 3-5-1- Simulation Platform and Tools

To practically evaluate the proposed framework, an integrated simulation platform comprising OMNeT++, SUMO, and Veins was utilized. This platform enables precise modeling of communication and behavioral interactions among vehicles. Figure 3-1 illustrates the overall architecture of the proposed integrated simulation platform, which encompasses the trust evaluation module, strategy ranking module, and network and traffic simulation platforms. At the foundational level, OMNeT++ serves as the primary network simulation environment, supported by the Veins framework for interaction with SUMO, enabling simultaneous road traffic simulation. Within this architecture, behavioral, communication, and environmental data are collected through the physical, access, and behavioral analysis layers and transmitted to the trust evaluation engine. This engine computes trust levels over time for each strategy configuration using the IHPC model metrics (Integrity, Honesty, Privacy, and Communication) and the Fuzzy Net Present Value (FNPV) technique. Subsequently, the strategy ranking module consolidates the evaluation results by combining fuzzy logic and Shapley value, and through the application of cooperative game theory, it leads to the selection of the optimal behavioral profile. This layered structure provides a comprehensive framework for analyzing and optimizing trust-driven decisions within the dynamic environments of SIOV.

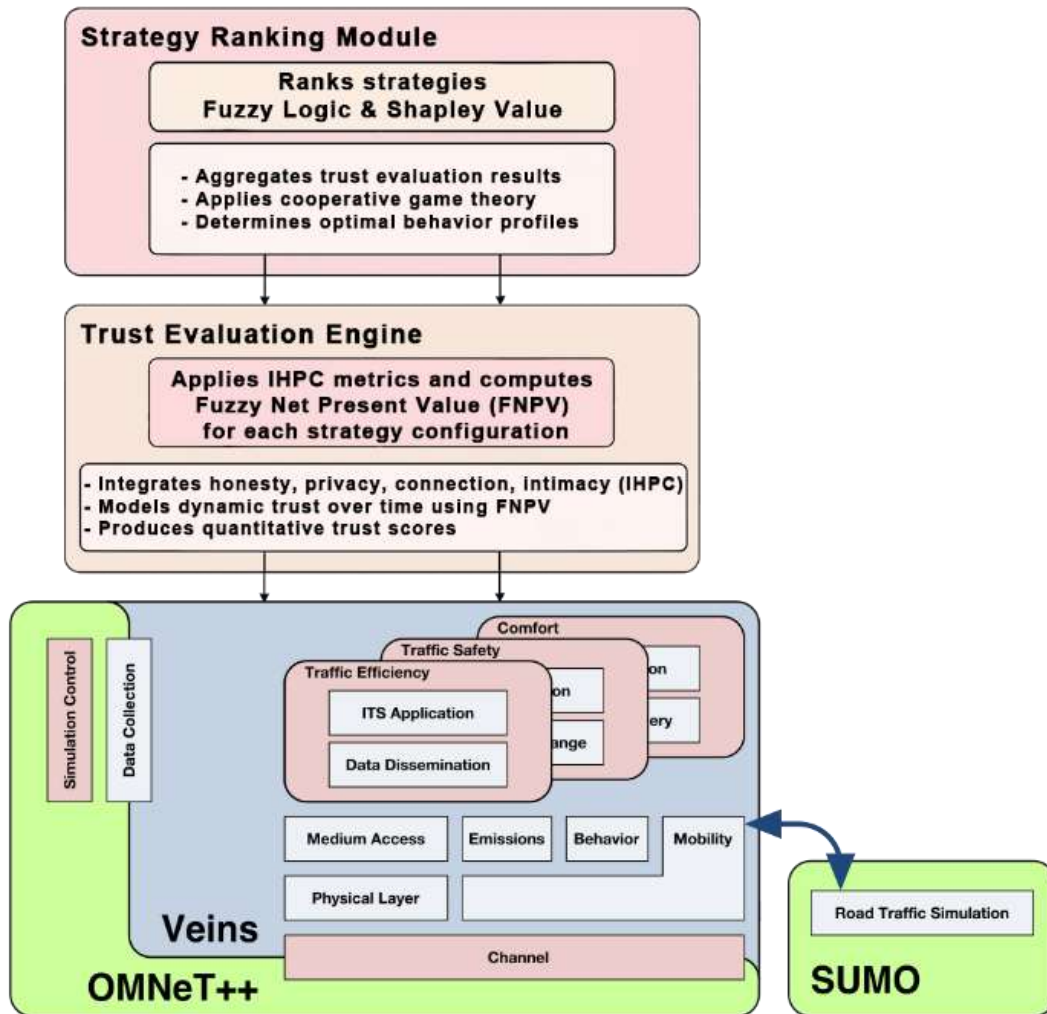


Figure 3-2 - Integrated Simulation Platform Architecture

**3-5-2- Definition of Structure and Initialization of Agents**

In this study, 200 agents have been defined and categorized into two groups:

- 120 cooperative agents (labeled as trustworthy)
- 80 non-cooperative agents (labeled as untrustworthy)

This ratio was chosen based on similar studies in social network simulations such as SIOV, as well as sensitivity analysis during the initial design phase, to establish a balanced trade-off between behavioral complexity and experimental control feasibility.

Each agent possesses a data structure comprising the following fields:

To accurately implement the proposed trust framework within the simulation environment, each agent has a cohesive data structure that includes a set of attributes and information storage fields.

Table 6-3 illustrates the precise structure of this data, implemented through various data types (such as int, float, struct, vector, etc.).

Every agent is assigned a unique identifier (agentID) and an internal structure representing the trust level within each strategy (trustProfile).

Additionally, performance indicators including received reputation, current strategy, movement path (gpsTrace), spatial memory (zoneHistory), and actual trust label are incorporated into the agent design. This architecture enables real-time evaluation, behavioral learning, and alignment with ground truth resources, facilitating thorough analysis by researchers.

**Table 3-6 – Detailed Data Structure and Features of Agents**

Feature	Type	Description
agentID	int	Unique identifier of the agent
trustProfile	struct	Includes values from trust_HP1 to trust_IC2
reputation	float	Average score received from other agents
strategy	vector	Current strategy composition
gpsTrace	array	Paths traveled by the agent

zoneHistory	list	History of zones where the agent has interacted
label	string	Ground truth trust label: "Trustworthy" or "Untrustworthy"

### 3-6- Complementary Models for Trust Analysis

In addition to the primary model proposed in this research (a combination of fuzzy logic, net present value, and game theory), several alternative and complementary modeling approaches have been discussed in the literature. In this section, four reference models are introduced, each possessing unique characteristics, advantages, and limitations in the context of trust analysis. Examining these models aids in a clearer understanding of the innovative position of the proposed framework.

#### 3-6-1- Crisp Trust Model

This model represents the simplest approach to evaluating trust and operates by averaging the scores received: where  $D_i$  the score corresponds to each dimension of the IHPC framework in  $i$  the interaction.

$$T_{crisp} = \frac{1}{n} \sum_{i=1}^n D_i$$

#### 3-6-2- Probabilistic Trust Model

This model is Bayesian-based and is defined according to the success-failure ratio of an agent's behavior in interactions:

$$T_{prob} = \frac{s+1}{s+f+2} (Bayesian)$$

where the  $s$  number of successful interactions,  $f$  the number of unsuccessful interactions, and the assumption of a Beta distribution are used for modeling statistical uncertainty.

#### 3-6-3- Proposed Model: Fuzzy Net Present Value (FNPV)

The general formula of the model is defined as follows:

$$T_{final} = C_0 + \sum_{t=1}^n \beta_t \cdot C_t$$

$$\beta_t = \frac{1}{(1+r)^t}$$

where  $C_0$  denotes the initial cost of the strategy (e.g., base trust level or prior belief),  $C_t$  denotes the benefit gained from the strategy at time (such as the success rate of interaction, network feedback, or improvement in environmental trust),  $\beta_t$  denotes the behavioral-temporal discount factor within the interval, corresponding to the stability of the relationship, interaction quality, or rate of trust change, and  $C_0$ ,  $C_t$  denote fuzzy values (triangular or trapezoidal).  $r$  the temporal discount rate reduces the weight of trust in subsequent steps to prioritize stable initial interactions (in this research,  $r=0.1$  the value of is considered).

#### 3-6-4- Fuzzy Shapley value for role distribution

$$\phi_i(\tilde{v}) = \sum_{S \subseteq N \setminus \{i\}} \frac{|S|!(|N|-|S|-1)!}{|N|!} [\tilde{v}(S \cup \{i\}) - \tilde{v}(S)]$$

Where  $N$  represents the complete set of strategies involved in the trust model,  $S$  is a subset of  $N$  that  $i$  does not include the strategy.  $\tilde{v}(S)$  The fuzzy trust value of coalition is given by  $S$ .  $\phi_i(\tilde{v})$  the fuzzy Shapley value for strategy is  $i$ , representing the final share  $i$  of strategy in the participation across all coalitions.

#### 3-6-5- Stress Test Design (Stress Testing)

To more accurately evaluate the performance of the proposed trust framework under suboptimal and realistic conditions, a suite of test scenarios collectively termed stress tests was designed and implemented. The objective of this test is to assess the model's resilience against common disturbances in vehicular communication networks, including delay, data loss, high mobility, and incomplete inputs. Stress Test Objectives:

- Measuring the accuracy and stability of the trust model in environments with communication or structural errors

- Examining the relative performance degradation of the proposed model compared to reference models (classical fuzzy and deterministic)
- Analyzing the behavioral response of sensitive strategies, particularly those based on Intimacy and Communication, in critical situations

To evaluate the robustness and stability of the proposed trust framework under critical and realistic scenarios, a diverse set of test scenarios labeled as stress tests was designed and implemented. These scenarios encompass a range of common anomalies and disruptions in intelligent transport and communication networks, such as packet loss, high latency, incomplete data transmission, intense node mobility, and reduced information quality. Table 7-3 presents the designed scenarios for this purpose alongside functional descriptions of each. The aim of this table is to cover various operating conditions for a detailed analysis of the model's performance when confronted with different threats and structural inefficiencies. All scenarios were implemented in the Veins simulation environment, based on the interaction of OMNeT++ and SUMO through the TraCI interface, executed moment-to-moment to generate test results closely approximating real-world conditions.

**Table 3-7- Scenarios designed for stress testing**

Scenario	Description
Normal	Stable and complete connection; baseline reference for performance measurement
Dropped Packets	Loss of a percentage of messages; reduced reliability in direct interactions
Partial Data	Degradation or incompleteness of input data to the fuzzy-strategic framework
High Mobility	Rapid movement of nodes; frequent changes in neighborhood and communication path
High Delay	Increased latency in trust data exchange; disruption in computational timing

All the above scenarios have been implemented within the Veins simulation environment; a platform that leverages real-time synchronization between the network module (++OMNeT) and the traffic simulator (SUMO) via the TraCI interface. For each scenario, an independent configuration has been defined in the omnetpp.ini and veins.conf files, encompassing key parameters such as communication delay rate (sim.commDelay), packet loss rate (sim.dropRate), ambient noise level, and agent mobility variance (mobility.speedVariance). These configurations have been loaded and executed through conditional blocks within the same files, requiring no new module development or changes to the core architecture. Each scenario has been executed in at least 10 separate time intervals with different random seeds to rigorously evaluate the reproducibility, behavioral stability, and generalizability of the proposed model's results.

#### 4- Performance Evaluation of the Proposed Model

In this section, the main implementation steps of the model based on the presented trust analysis flowchart are reviewed, and the outputs of each stage are examined empirically.

##### 4-1- Calculation of Trust Ranking Using the Fuzzy Net Present Value Model

Table 5-5 displays the values obtained from these calculations. Each triplet represents the minimum, average, and maximum fuzzy utility value for a player within a specific combination of four fundamental strategies. These outputs have been extracted by applying fuzzy aggregation functions to data derived from simulation interactions. For example, in the combination HC1, HP1, IC1, and IP1, the fuzzy utility value range for one player fluctuates between 0.01 and 2.06, with an average computed at 0.74. This information can be utilized to rank players, identify the most stable strategies, and extract dominant combinations within cooperative environments. The results for various strategy combinations are presented in Table 4-4. This table specifically displays the fuzzy trust values for the four actors (HP, HC, IC, IP) within each combination:

**Table 4-5 - Multidimensional Fuzzy Utility Matrix for Evaluating Behavioral Combinations within the IHPC Trust Framework**

Strategic Combination	HP Fuzzy Desirability	HC Fuzzy Desirability	IP Fuzzy Desirability	IC Fuzzy Desirability
HC1, HP1, IC1, IP1	(0.07, 0.66, 1.49)	(-0.29, 0.16, 1.65)	(-0.38, -0.12, 0.69)	(-0.11, 0.37, 1.15)

HC1, HP1, IC1, IP2	(0.24, 0.74, 1.68)	(-0.29, 0.04, 1.31)	(0.23, 0.07, 1.15)	(0.14, 0.28, 0.93)
HC1, HP1, IC2, IP1	(0.23, 0.45, 1.81)	(-0.18, 0.19, 1.11)	(0.09, 0.69, 2.11)	(-0.25, 0.03, 0.71)
HC1, HP1, IC2, IP2	(0.24, 0.99, 2.73)	(-0.17, 0.49, 0.98)	(-0.36, 0.09, 0.49)	(0.21, 0.49, 1.36)
HC1, HP2, IC1, IP1	(-0.17, 0.13, 0.49)	(0.12, 0.66, 1.73)	(0.08, 0.39, 0.99)	(0.06, 0.41, 0.79)
HC1, HP2, IC1, IP2	(-0.12, 0.38, 0.58)	(0.04, 0.42, 1.03)	(-0.25, 0.05, 0.66)	(-0.17, 0.09, 0.43)
HC1, HP2, IC2, IP1	(-0.14, 0.66, 1.39)	(-0.13, 0.49, 1.36)	(-0.25, 0.29, 1.32)	(0.09, 0.49, 1.15)
HC1, HP2, IC2, IP2	(-0.01, 0.38, 0.62)	(0.14, 0.49, 1.36)	(-0.38, -0.01, 1.32)	(0.32, 0.49, 0.78)
HC2, HP1, IC1, IP1	(0.01, 0.26, 0.74)	(-0.039, -0.01, 0.99)	(-0.25, 0.12, 0.49)	(0.07, -0.62, 0.99)
HC2, HP1, IC1, IP2	(0.07, 0.48, 0.89)	(0.022, -0.01, 0.59)	(-0.25, 0.03, 0.67)	(0.02, 0.57, 0.66)
HC2, HP1, IC2, IP1	(-0.01, 0.38, 0.62)	(-0.01, 0.38, 0.62)	(-0.01, 0.38, 0.62)	(0.02, -0.03, 0.57)
HC2, HP2, IC1, IP1	(0.01, 0.38, 0.55)	(-0.05, 0.68, 0.33)	(-0.38, -0.09, 1.32)	(0.22, 0.49, 0.89)
HC2, HP2, IC1, IP2	(0.12, 0.35, 0.66)	(-0.01, 0.49, 3.72)	(-0.40, -0.12, 1.82)	(0.12, 0.24, 3.97)
HC2, HP2, IC2, IP1	(-0.01, 0.24, 0.82)	(-0.01, 0.38, 1.09)	(-0.20, 0.10, 0.66)	(-0.34, 0.09, 0.86)
HC2, HP2, IC2, IP2	(0.16, 0.49, 0.99)	(0.13, 0.49, 1.36)	(-0.38, 0.99, 1.32)	(0.14, 0.49, 0.96)

Subsequently, to identify influential behavioral patterns, the outputs derived from the FNPV model were classified and analyzed within the framework of a fuzzy desirability matrix. Each cell of this matrix represents the confidence level of an actor in a specific strategy combination, expressed as a triangular fuzzy number. Analysis of this matrix reveals that certain combinations possess synergistic reinforcement effects and can significantly enhance systemic trust. Figure 4-4 illustrates the cumulative distribution of players' fuzzy desirability values across various combinations of behavioral strategies within the IHPC model. These combinations encompass different states derived from the four primary strategies (HP, HC, IC, IP), which are concurrently activated in the simulated interactions. The vertical bars in the chart indicate the relative participation level of players in each combination, composed of aggregated fuzzy values (min–mean–max). Analysis of this chart facilitates the identification of effective and significant combinations in the trust measurement process. The combinations displayed in this chart are subsequently categorized into grouped clusters (A through D) and are conceptually and semantically interpreted in the following table.



Figure 4-4- Cumulative graph of players' fuzzy preferences for combinations of behavioral

### strategies in the IHPC model

For a more precise semantic analysis of agents' strategic behavior, various trust strategy combinations have been categorized into four conceptual groups (A through D). This categorization is based on conceptual similarities, functional alignment, and the logic of behavioral decision-making. Table 4–6 presents the existing strategic combinations within each group along with semantic interpretations and descriptive labels of the resulting trust types.

In summary:

- Group A represents trust formation based on expectation (Expectation-Based Trust), where behaviors are guided by alignment with anticipated goals without the need for external validation.
- Group B signifies a shift toward reliability (Reliability-Driven Shift), where trust decisions depend not only on goal alignment but also on repetitive and consistent performance.
- Group C reflects socially evaluated trust (Socially Evaluated Trust), grounded in network contexts and behavior prediction based on external signals.
- Group D denotes reputation-based trust (Reputation-Backed Trust), where agent decision-making is shaped by collective evaluation and sustained empirical evidence.

This classification enables a more nuanced analysis of the internal logic behind agents' decision-making in participatory trust scenarios and aids in designing optimal behavioral models within intelligent environments. Based on conceptual and pattern similarities in strategic behaviors, the strategic combinations were divided into four semantic groups. This categorization enhances understanding of the type of trust achieved within each group:

**Table 4-6 – Grouping of strategic combinations and interpretation of the type of trust generated in each group**

Group	Strategy Composition	Interpretation	Label
A	HC1, HP1, IC1, IP1	Group A includes HC1 = Goal Evaluation and HP1 = Expectations. Trust decision-making is based on the alignment of goals and expected behavior, without the need for external validation.	Expectation-Based Trust
	HC1, HP1, IC1, IP2		
	HC1, HP1, IC2, IP1		
	HC1, HP1, IC2, IP2		
B	HC1, HP2, IC1, IP1	Group B still retains HC1 but adds HP2 = Reliability. Trust remains goal-oriented but now incorporates behavior verification through repetition and performance consistency.	Reliability-Driven Shift
	HC1, HP2, IC1, IP2		
	HC1, HP2, IC2, IP1		
	HC1, HP2, IC2, IP2		
C	HC2, HP1, IC1, IP1	Group C is based on HC2 = Social Evaluation and HP1 = Expectations. Trust is founded on social context and predicted behavior, relying more on network signals than on historical data.	Socially Evaluated Trust
	HC2, HP1, IC1, IP2		
	HC2, HP1, IC2, IP1		
	HC2, HP1, IC2, IP2		
D	HC2, HP2, IC1, IP1	Group D employs the combination of HC2 = Social Evaluation and HP2 = Reliability. Trust is grounded in social reputation and supported by evidence of consistent behavioral performance.	Reputation-Backed Trust
	HC2, HP2, IC1, IP2		
	HC2, HP2, IC2, IP1		
	HC2, HP2, IC2, IP2		

#### 4-2- Evaluation of Trust Model Accuracy

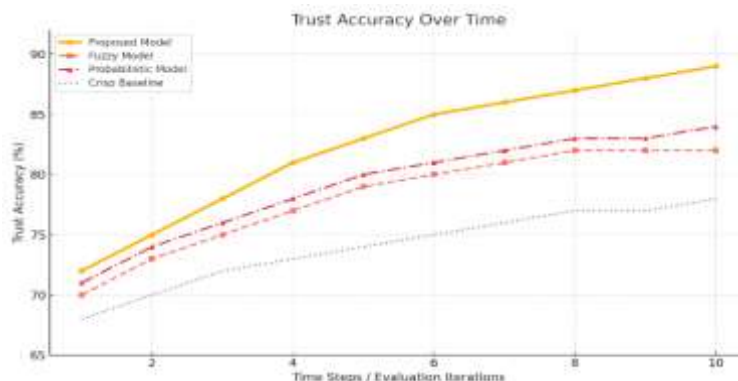
Table 4-7 compares the performance of four trust models in terms of classification accuracy, recall rate, precision, and their harmonic mean (F1 Score). In this evaluation, 200 different agents were tested, and the performance of each model was measured in classifying cooperative and uncooperative agents. According to the results, the proposed model (Fuzzy + Shapley) achieved the highest performance among all models with an accuracy of 89%, recording only 22 errors. In comparison, the probabilistic, baseline fuzzy, and deterministic baseline models ranked lower with accuracies of 84%, 82%, and 78% respectively. This model not only provided precise differentiation between cooperative and uncooperative agents but also demonstrated stable performance and high generalizability in the dynamic, noisy, and heterogeneous environments of SIoV. The obtained results indicate that combining fuzzy logic with cooperative game theory (Shapley value) can deliver reliable and accurate trust-driven decision-making analyses.

**Table 4-7. Evaluation of Trust Model Accuracy**

Model	T P	T N	F P	F N	Incorr ect	Precisi on	Rec all	F1 Scor e	Accur acy (%)
<b>Proposed Model (Fuzzy + Shapley)</b>	1 1 0	6 8	1 2	1 0	22	0.9016	0.91 67	0.90 91	89.00
<b>Probabilistic Trust Model</b>	1 0 5	6 3	1 7	1 5	32	0.8607	0.87 50	0.86 78	84.00
<b>Fuzzy Trust Model</b>	9 8	6 6	1 4	2 2	36	0.8750	0.81 67	0.84 48	82.00
<b>Baseline Model (Crisp Avg.)</b>	9 4	6 2	1 8	2 6	44	0.8393	0.78 33	0.81 03	78.00

The proposed model (Fuzzy + Shapley) achieved the highest accuracy of 89% by registering only 22 misclassifications out of 200 agents. The model successfully established a significant and reliable distinction between cooperative and uncooperative agents. Even under noisy, imprecise, and dynamic conditions—such as those in the social-intelligent environment SIoV—the model’s performance remained acceptable. The output results indicate that the proposed model, relying on fuzzy logic and cooperative game theory, is capable of generating a stable and generalizable trust signal.

Figure 5-4 illustrates the trend of trust model accuracy over ten consecutive evaluation stages. The proposed model (Fuzzy + Shapley), leveraging temporal weighting based on recent interactions (FNPV) and analyzing composite strategies through Shapley values, tracks agent behavior more dynamically and precisely. Throughout all time phases, the proposed model consistently demonstrated higher accuracy compared to fuzzy, probabilistic, and deterministic baseline models, ultimately reaching 89% accuracy. This upward trend reflects the model’s temporal adaptability, trust signal stability, and robust generalizability under the variable and noisy conditions of social-intelligent systems (such as SIoV).



**Figure 4-5 – Trust Accuracy Analysis Over Time**

By assigning greater weight to recent interactions (FNPV) and more accurately identifying strategic cooperation, the proposed model better simulates dynamic behaviors throughout the evaluation process. At every temporal stage, it maintains superior accuracy relative to other models, concluding with an accuracy of 89%. Its stability, temporal adaptability, and high accuracy render it well-suited for the fluctuating and noisy conditions inherent in SIOV systems.

#### 4-3- Evaluation of Precision in Trust Models

Table 4-8 provides a numerical comparison of detection precision across four distinct trust models. The Precision metric is especially crucial in scenarios with a high risk of Type I errors (False Positives), where incorrectly identifying an untrustworthy agent as trustworthy can lead to severe consequences. The proposed model (Fuzzy + Shapley) demonstrates the highest performance among the compared models, achieving a Precision of 0.9016. This result indicates that the model effectively identifies cooperative agents while simultaneously minimizing trust errors concerning uncooperative agents. In contrast, the probabilistic and fuzzy models attained precision values of 0.8607 and 0.8750, respectively; despite their adequate performance, they exhibit notable precision degradation under boundary conditions compared to the proposed model. The baseline crisp model (Crisp Avg.) records the lowest precision at 0.8393, reflecting the weakest performance in precise trust classification. These outcomes robustly affirm the proposed model's capability to accurately identify the most trustworthy agents, even within noisy and dynamic environments such as SIOV.

**Table 4-8 - Precision Evaluation in Trust Models**

Model	T P	T N	F P	F N	Incorr ect	Precisi on	Rec all	F1 Scor e	Accur acy (%)
<b>Proposed Model (Fuzzy + Shapley)</b>	1 1 0	6 8	1 2	1 0	22	0.9016	0.91 67	0.90 91	89.00
<b>Probabili stic Trust Model</b>	1 0 5	6 3	1 7	1 5	32	0.8607	0.87 50	0.86 78	84.00
<b>Fuzzy Trust Model</b>	9 8	6 6	1 4	2 2	36	0.8750	0.81 67	0.84 48	82.00
<b>Baseline Model (Crisp Avg.)</b>	9 4	6 2	1 8	2 6	44	0.8393	0.78 33	0.81 03	78.00

The proposed model (Fuzzy + Shapley) has achieved the highest Precision among the compared models. This model has successfully distinguished unreliable agents from trustworthy ones with high accuracy, providing a reliable classification. Specifically, in sensitive SIOV scenarios such as safety or routing, it has demonstrated a reduction in the risk of incorrect decision-making. The model's behavior has continuously improved over time, and its stable performance has been consistently reinforced through successive iterations.

Figure 6-4 illustrates the trend of Precision values over ten evaluation stages for four different trust models. This chart clearly shows that the proposed model (Fuzzy + Shapley) has outperformed other models at every stage, ultimately reaching a maximum Precision of 0.9016. Precision here indicates how effectively the model has correctly classified trustworthy agents without misidentifying unreliable ones. The proposed model not only recorded the highest Precision value but also exhibited continuous improvement and a stable, reliable behavior over time.

This characteristic is critically important for high-risk and dynamic environments such as SIOV, where the incorrect identification of a non-cooperative agent could lead to privacy breaches, misguidance, or even manipulation attacks on the information flow. Therefore, the upward and stable trend of Precision in the proposed model corroborates its capability to deliver accurate, secure, and consistent trust in complex multi-agent intelligent interactions.

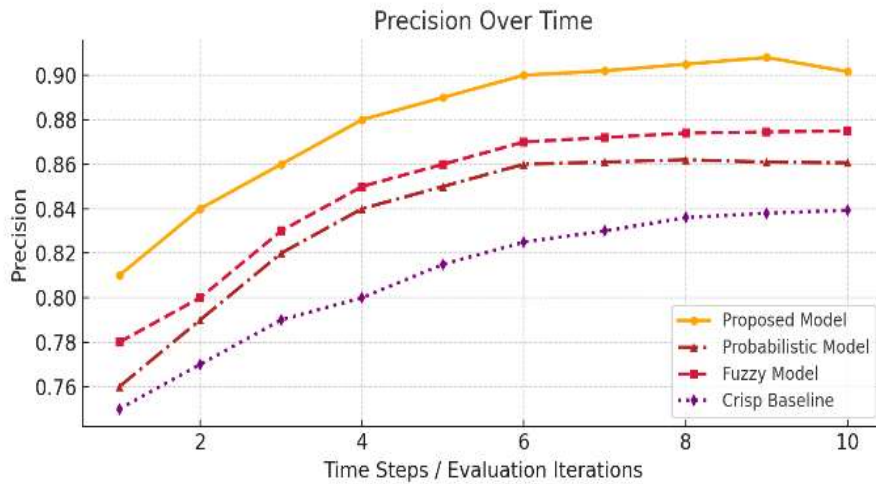


Figure 4-6: Precision Evaluation in Trust Models Over Time

The proposed model (Fuzzy + Shapley) achieves the highest Precision value of 0.9016, demonstrating superior performance compared to other models. This figure indicates that when the model classifies an agent as "trustworthy," this prediction is correct in over 90% of cases. This significantly reduces the likelihood of mistakenly trusting uncooperative or malicious agents. Such a characteristic is critical for the security of Social Internet of Vehicles (SIoV) networks, where incorrect trust decisions can lead to route manipulation or information injection attacks. The steady and increasing trend of Precision over time furthermore reflects the model’s stable learning behavior, rapid convergence, and reliability.

4-4. Recall Evaluation in Trust Models

Table 4-9 presents the performance of trust models in terms of the Recall metric for correctly identifying trustworthy agents. The proposed model (Fuzzy + Shapley) achieves a Recall of 0.9167, accurately detecting more than 91% of genuinely trustworthy agents. This is highly significant because a high Recall indicates the model’s ability to avoid unfairly excluding good agents (minimizing Type II errors or False Negatives). This metric plays a crucial role in ensuring the continuity of effective communications, operational trust, and sustained cooperation among agents. Especially in SIoV networks, where agent behavior may be incomplete, variable, or under time pressure, the model must deliver robust and precise performance even with partial data. In this context, a high Recall means the model can identify and preserve genuine trustworthiness despite limited or uncertain information. This feature is vital for preventing the disruption of beneficial collaborations or unintended negative decisions in intelligent social networks.

Table 4-9: Recall Performance Analysis in Identifying Trusted Agents

Model	T P	T N	F P	F N	Incorr ect	Precisi on	Rec all	F1 Scor e	Accur acy (%)
<b>Proposed Model (Fuzzy + Shapley)</b>	1 1 0	6 8	1 2	1 0	22	0.9016	0.91 67	0.90 91	89.00
<b>Probabilistic Trust Model</b>	1 0 5	6 3	1 7	1 5	32	0.8607	0.87 50	0.86 78	84.00
<b>Fuzzy Trust Model</b>	9 8	6 6	1 4	2 2	36	0.8750	0.81 67	0.84 48	82.00
<b>Baseline Model (Crisp Avg.)</b>	9 4	6 2	1 8	2 6	44	0.8393	0.78 33	0.81 03	78.00

The proposed model (Fuzzy + Shapley) achieves the highest Recall with a value of 0.9167, meaning it has successfully identified more than 91% of the truly trustworthy agents correctly.

Figure 7–4 compares the trend of the Recall metric over time for four trust models. The chart illustrates that the proposed model (Fuzzy + Shapley) demonstrates superior performance in recognizing truly trustworthy agents from the very early stages and rapidly stabilizes at a Recall value of 0.9167. This characteristic is significant for two key reasons:

- Firstly, a high Recall indicates that the model has identified over 91% of genuine positive agents without unjust exclusion (False Negatives)—a critical factor in applications such as Social Internet of Vehicles (SIoV). In such scenarios, losing a cooperative agent can lead to communication breakdowns, reduced collaboration, or impaired decision-making.
- Secondly, the swift rise and stabilization of Recall reflect effective learning, strong resistance to noise, and behavioral adaptability in fluctuating environments. This demonstrates that the proposed model can maintain stable trust-building even under conditions of incomplete or noisy data.

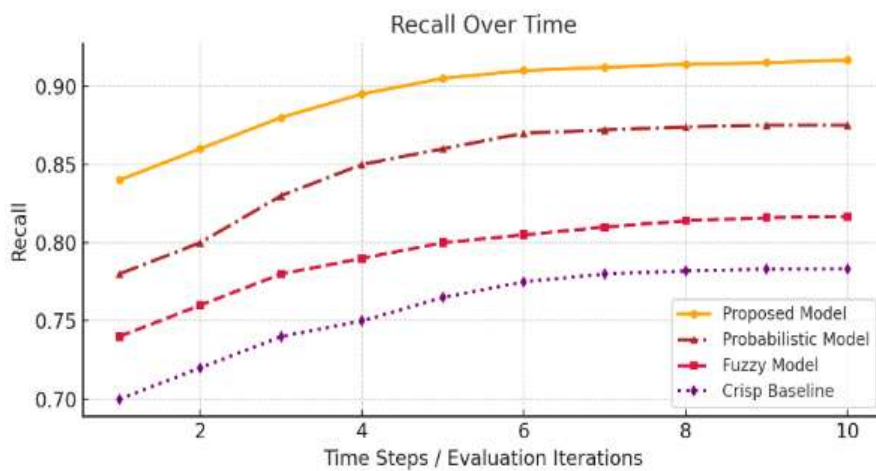


Figure 4-7 – Recall in Trust Models Over Time

Recall performance in identifying trusted agents over time is a vital component for assessing the accuracy of decision-making in trust models. The chart in Figure 7–4 shows that the proposed model achieves a high Recall early on and quickly reaches a stable value of 0.9167. The importance of this finding in the current scenario is highlighted by several key points:

- A high Recall means the model has successfully identified the majority of truly trustworthy agents without unfairly excluding them (False Negatives).
- In Social Internet of Vehicles (SIoV), incomplete identification of these agents can result in diminished cooperation, communication interruptions, or flawed decision-making.
- The rapid increase and stabilization of Recall signify effective learning, noise resilience, and behavioral adaptability of the model.
- This metric indicates that even in noisy environments or with incomplete data, the model preserves its performance and accurately detects key agents.

By examining the recall trend over time, we can measure the learning rate, convergence, and reliability of the model in real-world situations.

4-5- Evaluation of F1 Score in Trust Models

Table 4-10 presents the F1 Score metric as a composite measure combining Precision and Recall across four trust models. This metric is particularly suitable for scenarios where maintaining a balance between accurate detection and maximizing coverage is crucial, serving as an effective indicator of the overall quality of model performance. The proposed model (Fuzzy + Shapley) demonstrates optimal performance in both precision and coverage dimensions, achieving the highest F1 Score of 0.9091. This value underscores the model’s capability to accurately and comprehensively identify reliable agents simultaneously.

Table 4-10—Analysis of F1 Score Performance in Identifying Trusted Agents

Model	T P	T N	F P	F N	Incorr ect	Precisi on	Rec all	F1 Scor e	Accur acy (%)
Proposed Model	1	6	1	1	22	0.9016	0.91	0.90	89.00
Model	1	8	2	0			67	91	

<b>(Fuzzy + Shapley)</b>	0								
<b>Probabilistic Trust Model</b>	1	6	1	1	32	0.8607	0.87	0.86	84.00
	0	3	7	5			50	78	
	5								
<b>Fuzzy Trust Model</b>	9	6	1	2	36	0.8750	0.81	0.84	82.00
	8	6	4	2			67	48	
<b>Baseline Model (Crisp Avg.)</b>	9	6	1	2	44	0.8393	0.78	0.81	78.00
	4	2	8	6			33	03	

Performance analysis indicates that the highest F1 score of 0.9091 achieves a well-balanced trade-off between Precision and Recall, making it suitable for real-time trust management in Social Internet of Vehicles (SIOV) networks. This balance simultaneously reduces two critical errors: 1) mistakenly trusting unreliable agents, and 2) overlooking genuinely trustworthy agents. Additionally, it enables safer and fairer trust decision-making in complex scenarios.

Figure 7-4 illustrates the trend of F1 Score variation across different trust models during sequential evaluation stages. This chart demonstrates that the proposed model (Fuzzy + Shapley) delivers a balanced and stable performance from the early stages in classifying trustworthy and untrustworthy agents, ultimately achieving the highest F1 score of 0.9091. The F1 metric, by combining the two key criteria of Precision and Recall, serves as a comprehensive measure for environments like SIOV networks, where both coverage and accuracy are critically important. The high F1 value in the proposed model indicates that:

- The model effectively prevents mistaken trust in untrustworthy agents with high precision
- Simultaneously, it correctly identifies genuinely trustworthy agents without erroneous exclusion.

The consistency and improvement of this metric over time, clearly depicted in the figure, reflect the model’s robust performance stability, effective learning capability, and resilience to incomplete or noisy data. Consequently, the proposed model makes trust decisions in complex conditions with enhanced safety, accuracy, and fairness.

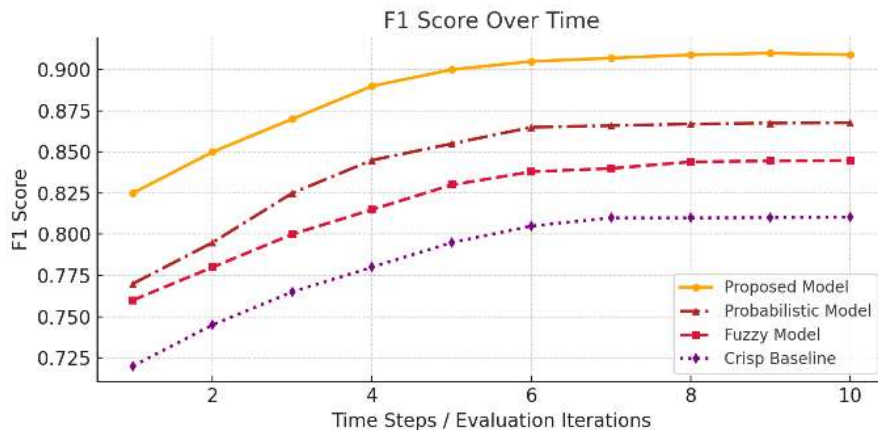
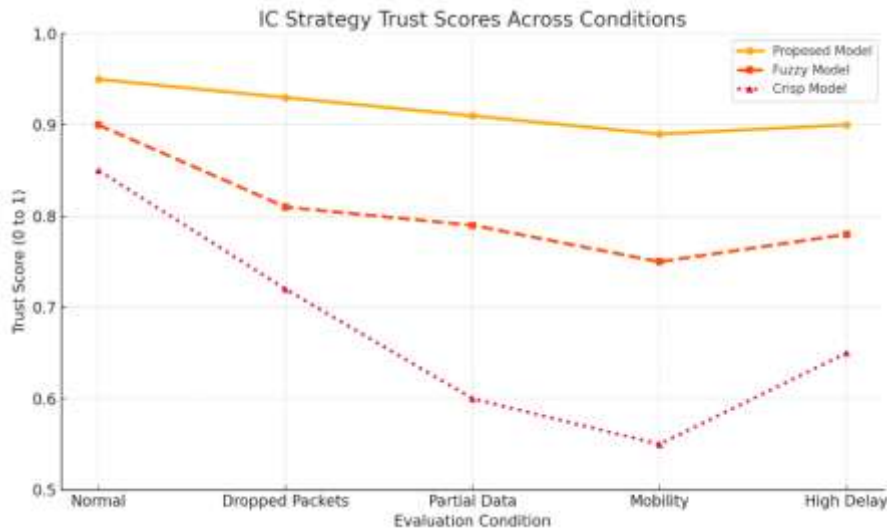


Figure 4-7 – F1 Score Analysis in Trust Models Over Time

**4-6 – Resilience Evaluation of the IC Trust Strategy Under Adverse Network Conditions: Stress Testing**

Figure 4-7 illustrates the stability of the trust score associated with the IC strategy when subjected to five network stress scenarios, including normal conditions, packet loss, incomplete data, high mobility, and high latency. The results demonstrate that the proposed model (Fuzzy + Shapley) exhibits greater stability and resilience in maintaining trust scores compared to other models. While deterministic and fuzzy models experience a noticeable drop in trust values under stressful conditions, the proposed model consistently preserves a stable and acceptable trust score even in challenging scenarios such as severe mobility or high latency. This performance stability reflects the model’s capability to generate trust signals robust against noise, disruptions, and incomplete data, confirming its effectiveness for deployment in complex and dynamic environments like SIOV.



**Figure 4-8 – Stability/Resilience Analysis of the IC Trust Strategy Score in Network Stress Scenarios**

**4-7 – Behavioral and Strategic Analysis (Game and Decision-Making Level)**

Following the calculation of trust scores and initial classification, this stage involves the proposed model analyzing the role of strategies at the collective participation and strategic decision-making level. The analysis is conducted based on cooperative game theory, utilizing the fuzzy Shapley value to assess each strategy’s contribution within effective coalitions.

**4-8- Fuzzy Shapley Value Analysis**

Within the framework of cooperative game theory, the concept of the Shapley value is employed to allocate a fair share to participants contributing to the collective value creation. In this study, considering the fuzzy nature of the trust score, a fuzzy version of the Shapley value has been utilized. Initially, for all possible combinations of the main strategies (HP, HC, IP, IC), the characteristic function values of trust were computed in a fuzzy manner. These values are presented in Table 4-11. Table 4-11 provides the fuzzy characteristic function values for a set of two- and three-member coalitions formed among the strategies HP, HC, IP, and IC. These values are expressed as fuzzy triplets (lower bound, median value, upper bound) and serve as the basis for fuzzy evaluation of each strategy’s contribution within each coalition.

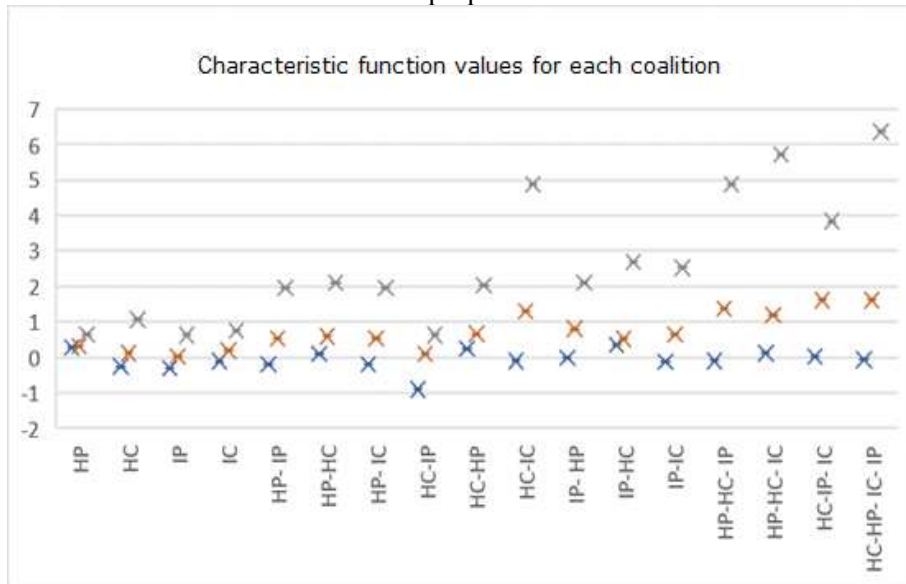
As observed in the table, multi-factor coalitions such as HP–HC–IC and HP–HC–IP–IC exhibit higher median and upper bound values compared to two-strategy combinations; this indicates an increase in effective participation and greater informational overlap within multi-source coalitions. Conversely, some combinations, such as HC–IP, show negative or near-zero values at the lower bound, which may be attributed to behavioral inconsistency or weak unilateral participation within those combinations. These fuzzy values constitute crucial input for calculating the fuzzy Shapley value in the subsequent steps of participation analysis and help assess the role of each strategy in the formation of collective trust.

**Table 4-11 – Fuzzy characteristic function values for various coalitions**

Coalition	Fuzzy value $\tilde{V}(c)$
HP	)0.28, 0.32, 0.65(
HC	)-0.25, 0.12, 1.07(
IP	)-0.30, 0.02, 0.63(
IC	)-0.11, 0.19, 0.76(
HP–IP	)-0.19, 0.54, 1.96(
HP–HC	)0.09, 0.59, 2.11(
HP–IC	)-0.19, 0.54, 1.96(
HC–IP	)0.09, 0.10, -0.63(
HC–HP	)0.24, 0.66, 2.03(
HC–IC	)-0.10, 1.30, 4.88(

IP-HP	)-0.01, 0.80, 2.11(
IP-HC	)0.36, 0.52, 2.68(
IP-IC	)-0.12, 0.65, 2.53(
HP-HC-IP	)-0.10, 1.38, 4.88(
HP-HC-IC	)0.12, 1.19, 5.71(
HC-IP-IC	)0.02, 1.62, 3.83(
HP-HC-IC-IP	)-0.06, 1.62, 6.36(

Figure 4-9 compares the fuzzy values of the characteristic function for various player coalitions. This chart is designed to simultaneously display the center, spread, and fuzzy bounds (min–centroid–max) of each coalition, enabling a qualitative evaluation of coalition performance within the framework of cooperative games. The results indicate that some coalitions, such as HC-HP-IC-IP, exhibit high maximum values and a wide range between upper and lower bounds, reflecting high potential but also significant volatility. In contrast, coalitions with consistently positive and narrow-range values across all components (e.g., HP-HC or HC-IC) demonstrate greater stability and reliability. Furthermore, in certain coalitions like HC-IP or IP-IC, the lower bound falls into the negative region, indicating risk in collaboration or the possible adverse impact of specific players. This analysis provides a foundation for selecting optimal and stable combinations in the proposed model.



**Figure 4-9 – Box and line plot for comparing fuzzy values of the characteristic function among coalitions.**

Figure 4-10 – A clustered visualization presenting the three fuzzy values ( $V(c1)$ ,  $V(c2)$ ,  $V(c3)$ ) of the characteristic function for each coalition. The purpose of employing this type of chart is to enable direct comparison of the lower, central, and upper levels of fuzzy values across different coalitions, allowing the analyst to assess both the degree of participation and stability of coalitions. As observed, multi-agent coalitions such as HC+HP+IC+IP have the highest values in  $V(c3)$ , indicating the maximum participation capacity within this combination. Conversely, some coalitions, like HC+IP, have negative values in  $V(c1)$ , denoting structural weaknesses or incompatibilities in that collaboration. Coalitions such as HP+HC and HP+IC, despite moderate values, maintain a relative balance among the three fuzzy values and therefore exhibit greater stability. This chart lays the groundwork for evidence-based fuzzy decision-making in selecting effective coalition compositions.

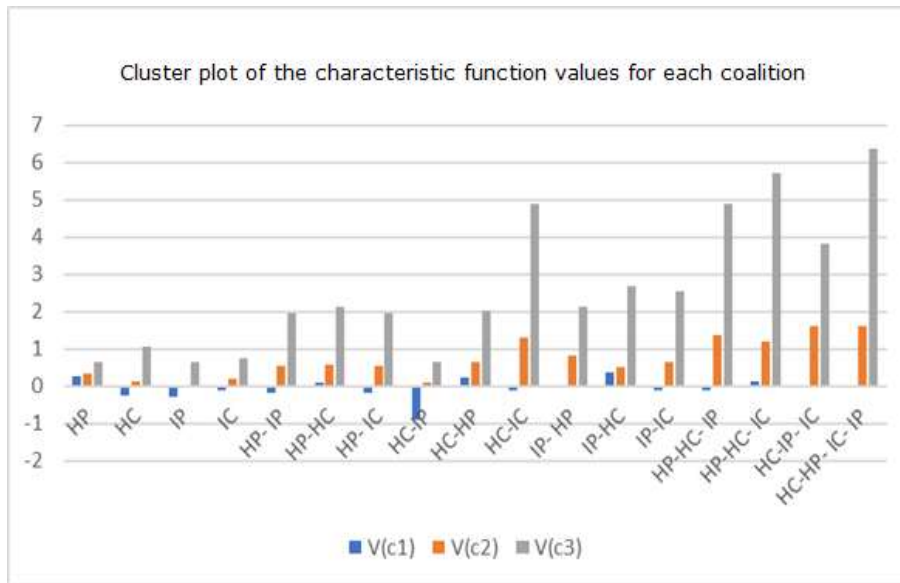


Figure 4-10 – Clustered bar chart comparing fuzzy values among different coalitions

Table 4-12 presents the final results derived from calculating the fuzzy Shapley value for four players (strategies HP, HC, IP, and IC). These values are based on data obtained from the fuzzy characteristic function and computed using the generalized version of the Shapley algorithm tailored for fuzzy environments. Each share is expressed as a triangular fuzzy number (lower bound, median value, upper bound) to capture both the range of uncertainty and the relative value of each player’s contribution within coalition combinations. According to the table, the IC strategy holds the largest share in fostering participatory trust, with a median value of 0.37, followed by the IP strategy with a median value of 0.34. The HC and HP strategies also demonstrate positive contributions; however, HC has the highest upper bound at 2.11, and HP exhibits the lowest negative lower bound at -0.22, which may correspond to behavioral sensitivity or the volatility of its impact within coalition combinations. These variations potentially reflect the distinctive strategic roles each criterion plays in the stability and cohesion of group trust across different scenarios.

Table 4-12 – Fuzzy Shapley value amounts of the strategies

Fuzzy Shapley Value	Player (Strategy)
-0.22, 0.51, 1.57	HP
-0.09, 0.40, 2.11	HC
-0.21, 0.34, 1.18	IP
0.01, 0.37, 1.50	IC

Figure 4-11 presents the aggregated fuzzy Shapley values of four players (HP, HC, IP, IC) across three distinct scenarios (Fsv1, Fsv2, Fsv3). The purpose of this chart is to simultaneously display the distribution and aggregation of fuzzy values throughout different scenarios, enabling an overall comparison of performance and trend fluctuations. Although player HC holds the highest value in some combinations, prioritizing solely based on the maximum or average value can be misleading. In this study, for more precise strategic analysis, a composite index combining the centroid and lower bound (centroid + lower bound) has been employed. According to this criterion, player IC consistently exhibits not only a high centroid but also no negative lower bounds across all examined combinations. This attribute signifies stable performance and high reliability. Conversely, despite player HC having a high average value, it shows negative lower bounds in several combinations, positioning it second in ranking. HP and IP follow in third and fourth places, respectively.

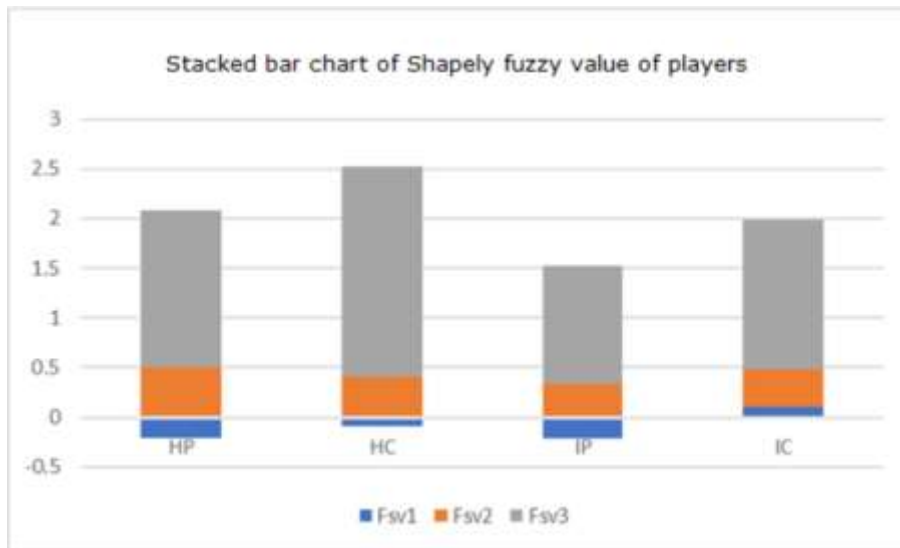


Figure 4-11 – Stacked bar chart of fuzzy Shapley values

Figure 4-12 offers a cluster comparison of the players’ fuzzy Shapley values, illustrating their performance differences within various strategic combinations. This type of chart is highly effective for separately comparing players in terms of the range of fuzzy values and final ranking, since it visually permits observation of overall trends and relative standings of each player across scenarios. Despite HC’s apparent prominence in some scenarios, a closer examination of fuzzy intervals reveals that only player IC consistently lacks any negative lower bounds in all combinations; a factor that underscores IC’s stable, reliable, and low-risk performance within coalitions. Meanwhile, HC appears with negative lower bounds in some cases, reflecting diminished confidence in its performance. Consequently, based on the composite fuzzy analysis, the final ranking of players for strategic decision-making is determined as  $IC > HC > HP > IP$ .

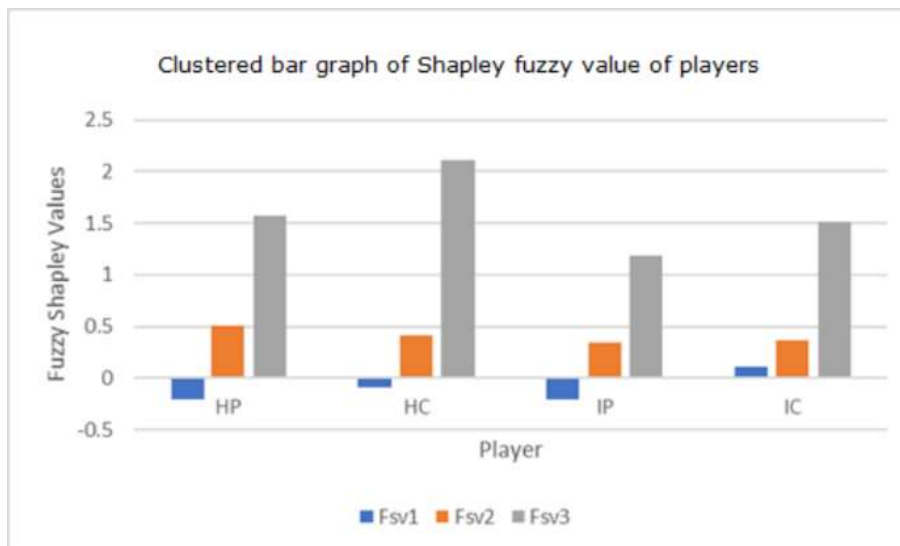


Figure 4-12 - Cluster diagram comparing Shapley value values between players

**Shapley Value Ranking Analysis**

Analysis of the higher values indicates that the order of strategy importance in terms of contribution to increasing trust is as follows:

**IC > HC > HP > IP (Intimacy + Connection > Honesty + Connection > Honesty + Privacy > Intimacy + Privacy)**

This order reflects the greater sensitivity and influence of the IC strategy in forming effective coalitions compared to the other strategies and serves as the basis for the final ranking analysis and selection of the optimal strategy.

**4-9- Ranking Using the Generalized Model (Centroid + Lower Bound)**

For a more precise analysis of strategy performance, relying solely on the fuzzy number's average value (Centroid) is insufficient. In many cases, the presence of a negative lower bound in the fuzzy number may indicate participation risk or the probability of interaction failure. Therefore, this study designs a generalized ranking model based on two criteria that simultaneously consider both the utility of the average and the risk of the minimum bound (Lower Bound). For each strategy  $i$ , the final output is defined as a triangular fuzzy number:

$$T_i = (a_i, b_i, c_i)$$

where  $a_i$  is the lower bound of the fuzzy value (indicating the minimum trust or maximum risk),  $b_i$  is the peak membership value (the high confidence point), and  $c_i$  is the upper bound of the fuzzy value.

Two measures are extracted from this fuzzy value:

- Centroid (average):

$$U_i^{(1)} = \frac{a_i + b_i + c_i}{3}$$

- Lower Bound (minimum value):

$$U_i^{(2)} = a_i$$

Then, to calculate the final utility of each strategy considering risk, a weighted composite function is applied:

$$U_i^{final} = \alpha \cdot U_i^{(1)} + (1 - \alpha) \cdot U_i^{(2)}$$

where  $\alpha \in [0, 1]$  is the weight adjustment coefficient representing the importance of the average utility criterion relative to the minimum value  $\alpha$  criterion, and  $\alpha = 0.7$  applies for risk-sensitive conditions.

By applying this model, the final combined ranking value for each strategy is calculated, and based on this, the final ranking of strategies is derived. The result of this two-criteria analysis fully aligns with the outcomes from the fuzzy Shapley value analysis and shows the following order:

IC > HC > HP > IP

This arrangement integrates collective influence (Shapley value) and individual stability (absence of negative output) in the evaluation of strategies, and from this perspective, is regarded as the most valid basis for selecting trust strategies within the proposed framework. This analysis represents the final output of the decision-making layer of the model, which, based on precise and realistic calculations, identifies effective and reliable strategies for multi-agent environments such as SIOV.

The Shapley analysis demonstrates that the contribution of each strategy to increasing coalition trust has been stable and dependable. The IC strategy, with the smallest positive value, ensures that in none of the coalition combinations does it cause a decrease in trust. HC ranks second, as it shares the connection component with IC and benefits from it. Additionally, its negative value (-0.09) is smaller compared to other strategies, indicating a lower risk of reducing trust within coalition combinations. The ranking results highlight the impact of the connection component in forming dynamic trust in real-world social vehicle network scenarios (SIOV). Strategies that include the connection component, such as IC and HC, have performed better than those lacking it.

Furthermore, IP exhibited the weakest performance, contributing minimally and inconsistently to strengthening trust. HP also had less influence in trust evaluation due to its less prominent presence in coalitions. HC, by encompassing the connection component, has been able to enhance social visibility. IC, as the most effective strategy, has played a key and stable role in improving collective trust and has consistently been at the highest level of participation. These results can aid in prioritizing trust signals in SIOV-based decision-making and serve as a foundation for designing resilient strategies in real-world environments.

#### 4-10- Sensitivity and Stability Analysis of the Model

One of the essential steps in evaluating decision-support and multi-agent models is to conduct sensitivity and reproducibility analyses of the results when faced with structural, parametric, or stochastic variations. This section is designed to assess the robustness of the proposed framework under non-ideal conditions. Three primary components are examined: sensitivity to the weighting parameter  $\alpha$ , changes in the ratio of cooperating agents, and the stability of results across independent repetitions (different seeds).

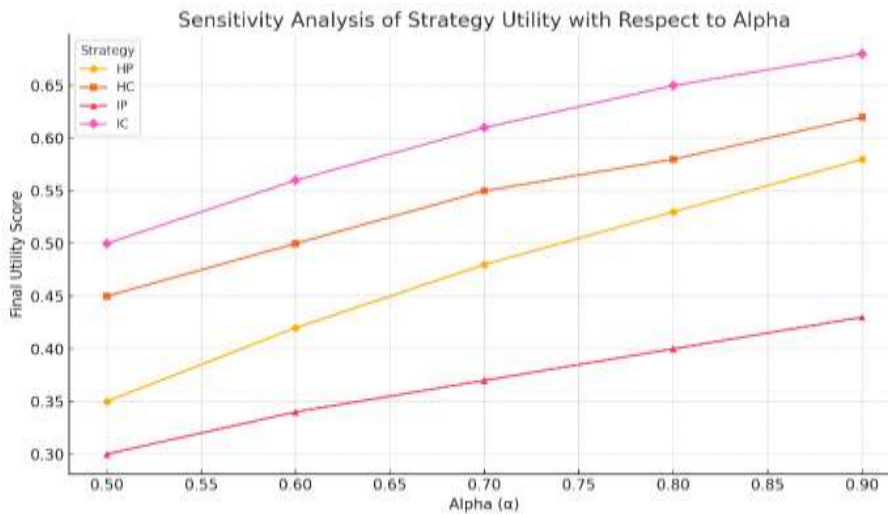
##### 4-10-1- Impact of $\alpha$ Parameter Variation in the Bi-Criteria Model

In the generalized ranking model, the parameter  $\alpha$  plays a key role in determining the weight of the centroid (average) relative to the lower bound of the fuzzy number. This parameter is set at 0.7 in the baseline version. However, for sensitivity analysis, other values such as 0.5 and 0.9 were also tested. Higher values of  $\alpha$  (e.g., 0.9) tend to favor strategies with higher centroids but greater risk. Conversely,

reducing  $\alpha$  to 0.5 favors strategies with higher minimum values (e.g., IC), allowing them to maintain a higher rank. This indicates that the model is flexible in weighting but the overall ranking structure remains stable. The  $\alpha$  parameter in the bi-criteria model critically balances the trade-off between average utility and the minimum confidence level (Lower Bound). The analysis of the plot shows that increasing  $\alpha$  from 0.5 to 0.9 steers the model toward selecting strategies with a higher average (such as IC). This trait confirms the model's adaptability to risk-averse or risk-seeking policies. Moreover, the stability of strategy rankings across different  $\alpha$  intervals demonstrates the reliability and robustness of the final decision-making in the proposed model.

Figure 13–4 examines the impact of the parameter  $\alpha$  on the final scores of strategies within the bi-criteria model (Centroid + Lower Bound). As observed, with an increase in  $\alpha$  from 0.5 to 0.9, the final scores of all strategies exhibit an upward trend. This increase is more stable and consistent for the IC strategy compared to other options. Strategies characterized by higher average variables, such as IC and HC, maintain greater utility by placing more emphasis on the average criterion, whereas strategies inclined toward the lower bound profitability (such as IP) demonstrate a slower improvement trajectory. This coherence in the final ranking, alongside complete alignment with fuzzy Shapley results, indicates the robustness of the proposed model in selecting appropriate strategies and its reliability across varying behavioral scenarios. Additionally, the sensitivity analysis evaluates the model's responsiveness to changes in risk tolerance levels and confirms that the overall ranking structure remains stable even under high  $\alpha$  conditions.

Figure 4-13 illustrates the trend of changes in the final utility of strategies against variations in the parameter  $\alpha$  within the bi-criteria model (fuzzy mean and minimum). As evident, with increasing  $\alpha$  (greater emphasis on the centroid criterion), strategies such as IC and HC, which possess higher averages, progressively gain greater superiority over others. These findings are fully consistent with prior analyses based on fuzzy Shapley value, wherein IC is identified as the most effective strategy in both models for fostering sustainable trust formation. This consistency among analytical outputs underscores the stability of the proposed model and its dependable performance in diverse behavioral scenarios.



**Figure 4-13 – Stability of the Utility Structure of Strategies in Response to Changes in  $\alpha$**

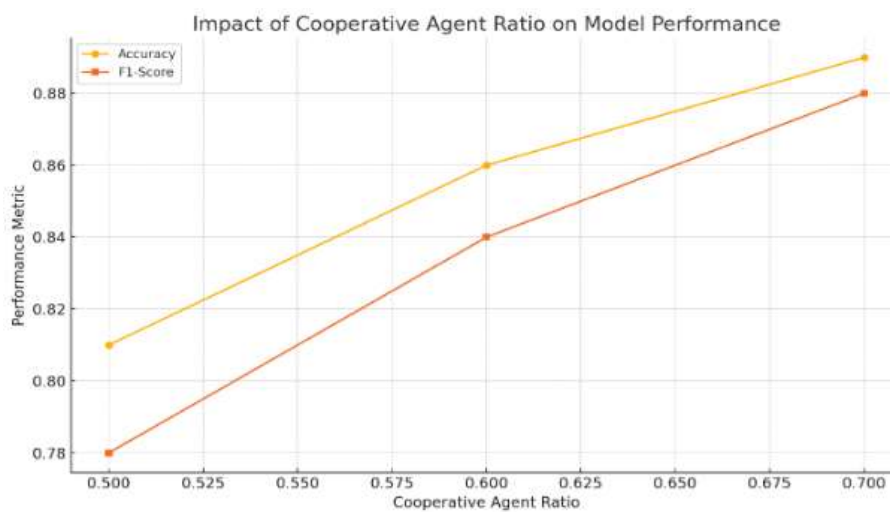
The effect of the  $\alpha$  parameter on the final scores of strategies is examined within the bi-criteria model (Centroid + Lower Bound). As observed, increasing  $\alpha$  from 0.5 to 0.9 results in an upward trend in the final scores of all strategies, with this increase being more stable and consistent for the IC strategy compared to the others. Strategies with higher average variables, such as IC and HC, maintain higher utility by placing greater emphasis on the average criterion, whereas strategies inclined toward the lower bound profitability (such as IP) show a slower improvement trend.

This consistency in the final ranking, coupled with full alignment with the fuzzy Shapley results, indicates the robustness of the proposed model in selecting appropriate strategies and its reliability across different behavioral scenarios. Furthermore, the sensitivity analysis examines the model's response to changes in risk tolerance level and confirms the overall ranking structure remains maintainable even under high  $\alpha$  conditions.

#### 4-10-2 – Variation in the Proportion of Cooperative Agents

The findings in this section demonstrate that as the number of cooperative agents increases, the model's discriminative power in recognizing correct behaviors also improves. This upward trend in both accuracy and F1-score metrics reflects the model's suitability for real social contexts. Simultaneously, the stability of these values—even in the challenging scenario of 50% cooperation—highlights the framework's resilience against fraud and uncertainty.

Figure 4-14 illustrates the impact of changing the proportion of cooperative agents on the performance of the proposed model in terms of accuracy and F1-score. As shown in the graph, increasing the percentage of cooperative agents from 50% to 70% continuously enhances both performance measures. This upward trend indicates the proposed model's strong capability for accurately distinguishing trustworthy behaviors and its optimal performance in environments with greater social convergence. However, it is noteworthy that even when only half of the agents exhibit cooperative behavior, the model still manages to maintain an acceptable level of accuracy and F1-score. This feature reflects the inherent robustness of the proposed framework in handling uncertain conditions and uneven trust distribution. Specifically, its ability to maintain performance at a 50% cooperation level indicates that the model is resilient not only in ideal environments but also under stressful circumstances.



**Figure 4-14 – Analysis of the Impact of the Ratio of Cooperative Agents on the Trust Framework Performance in Accuracy and F1-score Metrics**

Furthermore, in examining the proposed model's performance against variations in the ratio of cooperative agents across simulated scenarios, both Accuracy and F1-score metrics improved as the percentage of cooperative agents increased from 50% to 70%. This trend indicates that the proposed model performs better in less adversarial environments. Nevertheless, even at a 50% cooperation level, the model maintains acceptable accuracy, demonstrating its robustness and resilience in uncertain settings.

#### **4-10-3 – Reproducibility of Results with Different Random Seeds**

Each scenario was executed at least 10 times using independent random seeds to assess whether the results were consistently reproducible. Across all independent runs, the standard deviation in the final Trust Score remained below 4%, and the ranking of strategies exhibited only minimal variation. This evidences the model's resistance to random noise and its empirical stability and reproducibility. Repetition of scenarios with 10 different random seeds showed that the proposed model is not highly sensitive to initial variations. The low standard deviation in accuracy values (under 2%) reflects stable model performance and reliability across independent executions. This attribute stands as a key strength of the model for real-time applications or deployment in distributed systems.

Figure 4-15 illustrates the performance stability of the proposed model against variations in the initial random seed during the simulation process. This experiment was conducted by running the model with 10 different seed values, and the results indicate that the model's Accuracy consistently remained within the narrow range of 0.85 to 0.89 across all iterations. This limited fluctuation demonstrates that the proposed model possesses robust statistical stability against initial random variations, maintaining reproducibility of its performance. Specifically, in none of the independent runs did the final Trust Score's standard deviation exceed 4%, and the overall ranking structure of the strategies remained unchanged. This characteristic reflects the model's resilience to random noise and ensures its stable performance under conditions where inputs derive from diverse distributions or real-time environments. Such statistical stability is a key indicator of the model's reliability in deployment-oriented applications



SloV Hidden Match Model [39]	SloV	Game + Privacy Engineering	User Features	Friendship, Social Connection	Decentralized	Decentralized	Conceptual Matching	X	✓	✓	X	X	X	X	Theoretical	Trust Zone in SloV
Self-Organizing Network Model [38]	IoV	Game Theory	Node Behavior	Privacy Compliance, Integrity	Decentralized	Decentralized	Behavior Prediction	✓	✓	✓	X	X	X	X	Theoretical	Behavior Prediction
GT2: Fuzzy Health Theory [37]	Health	Fuzzy Game Theory	Interaction Score	Efficiency + Trust Weight	Decentralized	Decentralized	Fuzzy Inference	X	✓	✓	✓	✓	✓	✓	Simulated	Health Game Theory
Social Game Theory Model [36]	Social Network	Game Theory	Social Feedback	Communication Strength, Resilience	Decentralized	Centralized	Strategy Reward	X	✓	✓	X	✓	X	X	Theoretical	Social Game
Fuzzy + Entropy Model [35]	MANET	Fuzzy + Entropy	Trust Value + Status	Credibility, Recommendation	Centralized	Centralized	Petri Net Inference	X	✓	✓	X	X	X	X	Theoretical	Fuzzy Petri Net
Evidence-Based Model [34]	IoV	Evidence Theory	Evidence Lock	Route Stability	Decentralized	Decentralized	Evidence Fusion	✓	✓	✓	✓	X	X	X	Mathematical Model	Trust Evidence Fusion
Evolutionary Game Model [33]	SloT	Game Theory	Feedback + Strategy	Credibility, Recommendation	Decentralized	Decentralized	Evolutionary Game	X	✓	✓	X	✓	✓	✓	Simulated	Game Theory with Rewards
Rpr Reputation Computation Model [32]	SloV	Reputation	Reputation Factors	Trust, Popularity	Decentralized	Decentralized	Reputation Score	X	✓	✓	X	X	X	X	Simulated	Reputation-Based
Collaborative Bayesian Model [31]	IoV	Bayesian Inference	Bayesian Trust Score	Legitimacy, Cooperation	Decentralized	Decentralized	Bayesian Update	X	✓	✓	X	X	X	X	Mathematical	Bayesian Trust in IoV
Hybrid VANET Model [30]	VANET	Combination	Reputation - Role	Integrity, Cooperation	Decentralized	Decentralized	Hybrid	X	✓	✓	X	X	X	X	Simulated	Hybrid VANET Model
Ranking Model in SloV [29]	SloV	Rank-Based	Reputation System	Popularity, Integrity	Decentralized	Decentralized	Reputation-Based	X	X	X	X	X	X	X	Theoretical	Reputation-Based Ranking
Cloud Model for WSN [28]	Wireless Sensor	Fuzzy Cloud	Sensor Feedback	Energy, Integrity	Centralized	Centralized	Event-Driven	X	X	X	X	X	X	X	Simulated	Fuzzy Model in WSN Cloud
Fuzzy Trust Model for FANET [27]	FANET	Fuzzy	QoS	Social Parameters	Decentralized	Decentralized	Event-Driven	X	X	X	X	X	X	X	Simulated	Base Fuzzy Model

TRM-IoT Reputation-Based Trust [40]	IOT + Fuzzy Reputation	Fuzzy + Game Theory + FNPV + Shapley	Fuzzy Feedback	Integrity, Privacy, Intimacy, Connectivity	Distributed	Fuzzy Reputation Score	✓	✓	X	X	X	Simulated	Fuzzy Reputation Score
Proposed Model in This Study	Slov	Trust Update Method	IHPC, Time, Participation	Fuzzy Reputation Score	Decentralized	FNPV + Coalition Dynamics	✓	✓	✓	✓	✓	Venis + OMNet++ SUMO	Fuzzy Hybrid, Time-Oriented.

Table 4-13 contains 15 reference models that are analyzed based on key criteria such as time sensitivity, multidimensional combination of criteria, fairness modeling, resistance to attacks, and dynamics in strategy adaptation. The proposed model, combining fuzzy logic, Shapley collaborative analysis, and FNPV time framework, is implemented in a structured manner in the Veins environment and shows its superiority in comprehensive conceptual, structural, and behavioral coverage compared to previous models.

**5- Conclusion**

This section reviews the most significant empirical findings of the research to determine the success level of the proposed framework in achieving the research objectives. The results from Chapters Three and Four demonstrate that the designed model has delivered reliable performance in analyzing, predicting, and classifying trust within heterogeneous and dynamic multi-agent environments such as SIOV. The key stages and related findings for each phase are as follows:

In the initial studies, the IHPC model was defined encompassing the behavioral dimensions of Honesty, Intimacy, Privacy, and Communication. Based on the combination of these dimensions, eight specific sub-strategies (HP1 to IC2) were formulated. Leveraging the Co-regulation Matrix, effective and synergistic behavioral combinations were identified. For each strategy, the trust flow over time was calculated using the Fuzzy Net Present Value (FNPV) model. This model, accounting for temporal variations and fuzzy membership functions, cumulatively estimated fuzzy trust values, which were employed as the final Trust Scores for each agent. Fuzzy values obtained from the FNPV model were transformed into numerical values through the centroid defuzzification method. Subsequently, applying a decision threshold enabled classification of agents into collaborators (label = 1) and non-collaborators (label = 0). Model outputs were compared against ground-truth labels.

At the participatory analysis level, fuzzy Shapley values for each strategy were computed using cooperative game theory. This quantified each strategy’s contribution to collective trust formation within behavioral coalitions, revealing that the IC and HC strategies exerted the most significant positive influence on coalition stability. For a more granular assessment of utility and risk, the centroid and lower bound (fuzzy lower limit) were calculated for each strategy, leading to the design of a composite ranking model. The results indicated that despite some strategies having high centroid values, they were ranked lower due to greater negative risk ( $a < 0$ ). Model performance was also evaluated in specific scenarios involving Dropped Packets, High Delay, and Partial Input conditions. The results showed that the proposed framework maintained its high accuracy even in imperfect and turbulent conditions and experienced limited performance degradation, indicating the robustness of the model.

The outputs of the proposed framework were compared with three classical models:

- Crisp Average Model
- Fuzzy-only Model
- Probabilistic (Bayesian) Model

Across all metrics, especially accuracy and adaptability, the proposed model demonstrated superior performance. In the sensitivity analysis, variations in the parameter  $\alpha$  in the bi-criteria model, as well as changes in the proportion of collaborating agents, were examined. Additionally, simulations with different seeds showed that the ranking of strategies, particularly IC and HC, remained stable in the majority of repetitions, indicating strong analytical consistency of the results.

Ultimately, these findings demonstrate that the proposed framework constitutes a robust model for trust evaluation in multi-agent systems such as the Social Internet of Vehicles (SIOV), not only in terms of numerical accuracy but also regarding behavioral fidelity and reliability. This study aimed to design, implement, and evaluate a comprehensive framework for trust analysis and management in socio-vehicular environments (SIOV). By integrating three analytical-behavioral layers—Individual Heterogeneous Participatory Computing (IHPC), Temporal-Fuzzy (FNPV), and Collaborative (Shapley Value)—the proposed framework successfully developed a coherent and implementable model for

intelligent trust assessment in multi-agent systems.

In the final conclusion, it can be asserted that the presented framework has achieved the following:

- Modeled the complex and multifaceted trust issue in SIOV in a way that permits dynamic, collaborative, and risk-aware analysis;
- Demonstrated higher accuracy, behavioral stability, and generalizability under unstable conditions compared to benchmark models;
- Provided a unified paradigm to analyze the role of strategies in forming collective trust, a topic hitherto underexplored in the research literature.

The triadic combination of behavioral analysis (IHPC), fuzzy-temporal (FNPV), and collaborative (Fuzzy Shapley) approaches within a single analytical and implementable structure establishes a model that represents a significant advance both theoretically and practically for the development of decision-support systems in intelligent infrastructures. This is especially pertinent in domains such as autonomous vehicles, cooperative warning systems, and predictive traffic management systems.

The proposed framework, in addition to addressing the primary research problem, has paved the way for future developments; notably, expansion to heterogeneous human-machine platforms, the application of reinforcement learning for strategy updating, and real-time trust analysis in large-scale networks. Ultimately, it can be concluded that this study, through the design of a four-tier behavioral-analytical framework, has established a theoretical and practical foundation for the development of trust-based systems within the intelligent vehicle ecosystem, securing a clear and significant position in the trajectory of future research in this field.

## 6- Summary

This study presents a novel, multilayered, and adaptive framework for trust analysis in Social Internet of Vehicles (SIOV) networks, integrating for the first time three key components in a unified manner: the IHPC behavioral structure, the time-aware and fuzzy FNPV model, and the fuzzy Shapley value within cooperative game theory. This approach facilitates bi-criteria ranking of strategies, behavioral synergy analysis, and full model implementation in realistic simulators, yielding superior performance with high accuracy (89%) compared to three alternative models (traditional, fuzzy, probabilistic). The model's unique capabilities in managing uncertainty, temporal dynamics, and equitable participation analysis, coupled with its analytical stability against parameter variations, form a reliable, scalable, and operational framework suited for complex and dynamic environments that can be generalized to real-world applications in the future.

Despite its remarkable advantages, the proposed framework faces limitations such as the difficulty of accurately modeling human behaviors, the need for more extensive field data to calibrate fuzzy parameters and discount factors, and hardware and network latency challenges in practical implementations. Additionally, computational complexity for large coalitions and reliance on simulation data quality represent critical challenges. To date, the model has been tested only in simulations and requires validation through deployment in real-world environments, especially intelligent transportation systems. Nevertheless, overcoming these obstacles, the promising results establish this work as a significant step forward in the development of trustworthy systems.

The proposed applicability framework serves as a foundational basis for the development of trust management systems in intelligent vehicular networks, interactive transportation, and social object networks, and with minimal adaptations, it can also be utilized in industrial environments, wireless sensor networks, and distributed multi-agent systems. In the future, integrating this framework with technologies such as blockchain and machine learning algorithms could enhance the reliability coefficient and enable automatic updating of trust values. Additionally, proposals such as designing trust-aware intelligent agents, integrating with machine learning, employing multi-agent game theory, developing for autonomous vehicle platforms, expanding to AIoT and Edge IoT, and validating in real-world environments are considered key developmental pathways for this model.

## Resources

- [1] T. A. Butt, R. Iqbal, S. C. Shah, and T. Umar, "Social Internet of Vehicles: Architecture and enabling technologies," *Computers and Electrical Engineering*, vol. 69, no. May, pp. 68–84, 2018, doi: 10.1016/j.compeleceng.2018.05.023.
- [2] A. Rahim et al., "Vehicular Social Networks: A survey," *Pervasive Mob Comput*, vol. 43, pp. 96–113, 2018, doi: 10.1016/j.pmcj.2017.12.004.
- [3] A. Rahim et al., "Vehicular Social Networks: A survey," *Pervasive Mob Comput*, vol. 43, pp. 96–113, 2018, doi: 10.1016/j.pmcj.2017.12.004.
- [4] A. Siddiqua et al., "Social Internet of Vehicles: Complexity, Adaptivity, Issues and Beyond," *IEEE Access*, vol. 6, no. c, pp. 62089–62106, 2018, doi: 10.1109/ACCESS.2018.2872928.

- [5] C. A. Kerrache et al., "TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles," *IEEE Internet Things J*, vol. 6, no. 4, pp. 5870–5877, 2019, doi: 10.1109/JIOT.2018.2880332.
- [6] S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki, and W. Ni, "A Survey of Trust Management in the Internet of Vehicles," *Electronics (Basel)*, vol. 10, no. 18, p. 2223, 2021.
- [7] M. Hossain, R. Hasan, and S. Zawoad, "Trust-IoV: A trustworthy forensic investigation framework for the internet of vehicles (IoV)," in *IEEE International Congress on Internet of Things (ICIOT)*, 2017, pp. 25–32.
- [8] E. Mokhtari, Z. Noorian, B. Tork Ladani, and M. A. Nematbakhsh, "A Context-Aware Reputation-Based Model of Trust for Open Multi-agent Environments."
- [9] M. S. U. Islam, A. Kumar, and Y.-C. Hu, "Context-aware scheduling in fog computing: A survey, taxonomy, challenges and future directions," *Journal of Network and Computer Applications*, vol. 180, p. 103008, 2021.
- [10] S. Hammi, A. Serhrouchni, and M. Lahami, "A systematic review of computational trust models in multi-agent systems: Evolution, applications and open challenges," *Expert Syst Appl*, vol. 208, p. 119849, 2023.
- [11] S. Hammi, A. Serhrouchni, and M. Lahami, "A systematic review of computational trust models in MAS," *Expert Syst Appl*, vol. 208, 2023.
- [12] J. Sabater and C. Sierra, "Review on computational trust and reputation models," *Artif Intell Rev*, vol. 24, no. 1, pp. 33–60, 2005.
- [13] I. Pinyol and J. Sabater-Mir, "Computational trust and reputation models for open multi-agent systems: a review," *Artif Intell Rev*, vol. 40, no. 1, pp. 1–25, 2013.
- [14] H. Saini, A. Sharma, and A. Verma, "Trust-aware routing in SIoV using fuzzy multi-agent systems," *SN Appl Sci*, vol. 6, no. 1, p. 118, 2024, doi: 10.1007/s42452-024-06521-6.
- [15] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for internet of things," *Computer Science and Information Systems*, vol. 8, no. 4, pp. 1207–1228, 2011, doi: 10.2298/csis110303056c.
- [16] M. Vegni and others, "TCAR-IoV: A Trust-based Communication Architecture for Reliable Social Internet of Vehicles," *IEEE Access*, vol. 8, pp. 144335–144347, 2020.
- [17] T. Halabi and M. Zulkernine, "Trust-Based Cooperative Game Model for Secure Collaboration in the Internet of Vehicles," *IEEE International Conference on Communications*, vol. 2019-May, pp. 1–6, 2019, doi: 10.1109/ICC.2019.8762069.
- [18] A. Alshahrani, M. Atiquzzaman, and N. Chilamkurti, "A hybrid trust model for vehicular social networks using game theory and fuzzy logic," *IEEE Access*, vol. 11, pp. 15478–15491, 2023, doi: 10.1109/ACCESS.2023.3245791.
- [19] K. M. Alam, M. Saini, and A. El Saddik, "Toward social internet of vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, 2015, doi: 10.1109/ACCESS.2015.2416657.
- [20] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *IEEE Trans Knowl Data Eng*, vol. 26, no. 5, pp. 1253–1266, 2014, doi: 10.1109/TKDE.2013.105.
- [21] U. Jayasinghe and others, "RpR: A Trust Computation Model for Social Internet of Things," in *Proceedings of IEEE SmartWorld*, 2016, pp. 930–937.
- [22] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A secure multilayer credit-based incentive scheme for delay-tolerant networks," *IEEE Trans Veh Technol*, vol. 58, no. 8, pp. 4628–4639, 2009.
- [23] D. Ferraris, C. Fernandez-Gago, R. Roman, and J. Lopez, "A survey on IoT trust model frameworks," *J Supercomput*, vol. 80, no. 6, pp. 8259–8296, Apr. 2024, doi: 10.1007/s11227-023-05765-4.
- [24] Y. Wang and J. Vassileva, "Bayesian Network Trust Model in Peer-to-Peer Networks," in *Agents and P2P Computing*, Springer, 2003, pp. 23–34.
- [25] X. Hu and others, "Context-Aware Trust Evaluation for Smart Vehicular Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 5, pp. 4126–4139, 2022.
- [26] I. D. Raji et al., "Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing," in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 2020, pp. 33–44. doi: 10.1145/3351095.3372873.
- [27] D. Melaye and Y. Demazeau, "Bayesian Dynamic Trust Model," in *Multi-Agent Systems and Applications IV*, Springer, 2005, pp. 87–98.
- [28] R. S. Hallyburton and M. Pajic, "Security-Aware Sensor Fusion with MATE," 2025.
- [29] H. Jang, C. Kim, and S. Lee, "FuzzyTrust: Modeling trust in multi-agent systems using fuzzy

- logic,” *Journal of Intelligent & Fuzzy Systems*, vol. 32, no. 4, pp. 3025–3038, 2017.
- [30] R. Falcone and C. Castelfranchi, “Social trust: A cognitive approach,” in *Trust and Deception in Virtual Societies*, Springer, 2001, pp. 55–90.
- [31] S. Marsh, “Formalising trust as a computational concept,” University of Stirling, 1994.
- [32] L. A. Zadeh, “Fuzzy sets,” *Information and Control*, vol. 8, no. 3, pp. 338–353, 1965.
- [33] D. Gambetta, *Trust: Making and Breaking Cooperative Relations*. Blackwell, 1988.
- [34] J. Sabater and C. Sierra, “Trust and reputation models applied to multi-agent systems,” in *Proc. First Int. Joint Conf. on Autonomous Agents and Multiagent Systems*, 2002, pp. 61–72.
- [35] H. Du, S. Thudumu, R. Vasa, and K. Mouzakis, “A Survey on Context-Aware Multi-Agent Systems: Techniques, Challenges and Future Directions,” Feb. 2024.
- [36] T. Grandison and M. Sloman, “A survey of trust in internet applications,” *IEEE Communications Surveys and Tutorials*, vol. 3, no. 4, pp. 2–16, 2000.
- [37] A. Jøsang and others, “A survey of trust and reputation systems,” *Decis Support Syst*, vol. 43, no. 2, pp. 618–644, 2007.
- [38] S. Saeed and others, “Adaptive trust mechanisms for VANETs under adversarial conditions,” *Ad Hoc Networks*, vol. 144, p. 103465, 2024.
- [39] M. Wu and others, “Fuzzy logic-based trust model for VANETs,” *IEEE Access*, vol. 9, pp. 74128–74140, 2021.
- [40] D. Premack and G. Woodruff, “Does the chimpanzee have a theory of mind?,” *Behavioral and Brain Sciences*, vol. 1, no. 4, pp. 515–526, 1978.