International Journal of Multiphysics
Volume 18, No. 4, 2024
ISSN: 1750-9548

Providing a Trustworthy Framework on the Social Internet of Vehicles Based on Fuzzy Logic and Game Theory

Alireza Seddighi[1], Seyyed Amir Asghari[2*], Morteza Romoozi[3], Hamideh Babaei[4]

[1] PhD student in computer engineering, software systems, Department of Computer Engineering, Qom Branch, Islamic Azad University, Qom, Iran.
[2]Corresponding author, Associate Professor, Department of Electrical and Computer Engineering, Kharazmi University, Tehran, Iran.
[3]Assistant Professor, Department of Computer Engineering, Kashan Branch, Islamic Azad University, Kashan, Iran.
[4]Assistant Professor, Department of Computer Engineering, Naragh Branch, Islamic Azad University, Naragh, Iran.
*Corresponding author

Abstract

The Social Internet of Vehicles is a new generation of the Social Internet of Things, and trust in it is derived from the social relationship between entities and social vehicles. It is measured by criteria such as intimacy, honesty, privacy, and communication. The structure of trust depends on what is considered in trust calculations and on various factors such as popularity, environment, goals, expectations, social connections, and evaluation in a reasonable timeframe. The challenges of managing trust in the Social Internet of Vehicles include factors like strategies related to public reputation, local knowledge, social connections, trustworthiness, and privacy. This article aims to provide a trustworthy framework in the Social Internet of Vehicles through concepts such as fuzzy logic and game theory (Shapley value calculation). Due to the collaborative nature of entities (players), a cooperative gaming approach has been used to implement the strategies of the proposed model.

Keywords: Cooperative Games, Fuzzy Logic, Game Theory, Shapley Value, Trust

Introduction

Social Internet of Vehicles (SIoV) is a new and emerging generation in today's mobile computing field. The SIoV can be considered a derivative of several networks without infrastructure, networks such as the Social Internet of Things, networks without infrastructure of vehicles, and Internet of Vehicles [1]. The term “social” refers to the interaction of heterogeneous and unbalanced devices with different operating systems and different operating capacities; the purpose of creating heterogeneous networks is to share information with each other and ultimately obtain beneficial results for the environment and humankind, as well as provide sustainable transportation services and intelligent programs to its users [2]. In the SIoV, complex and dynamic data from vehicles, humans, and the environment are captured, sent, and processed in real-time to enable a wide range of services, such as improving driving conditions and road safety, traffic management, pollution control, and vehicle maintenance [3]. Therefore, the correctness and accuracy of this data is vital for the performance and quality of the services provided. Security issues are a big challenge in this network because these systems are vulnerable to different threats. Because of the highly dynamic nature and instantaneous interactions between vehicles and other entities, traditional security solutions for protecting data integrity based around centralized security infrastructures cannot be beneficial. Therefore, the security mechanisms used in these systems must be distributed, which do not rely on central institutions and is resistant to internal attacks and their destructive effects [4-5]. The concept of trust has been proposed as a measure to secure connected entities [6]. Trust between entities means having confidence in the exchange of information through the types of communication available in this type of network [7]. Golbeck introduced the concept of social trust on a sociological basis and introduced trust as "a commitment to act based on the belief that the person's future actions will lead to a good outcome" [8]. Golbeck sees social networks as an operating system for establishing mutual trust between individuals [9]. The issue of trust in the SIoV has been well studied in social networks [10]. The following will examine the importance and necessity of trust management in the SIoV. Relativity of trust and evaluation of the performance of predicted trust management models against different attacks and specific challenges are of significant importance [11]. In-vehicle networks also require precise processing of complex data to assess node reliability as well as early detection of hostile nodes [12]. As has been mentioned, the relativity of calculations and the examination of trust is a complex matter that will require cost-effective approaches and methods for accurate calculations. A widely used approach in the field of trust calculations is the use of fuzzy logic [13]. Another approach used in trust calculations is the use of game theory methods. In this regard, [14] proposes a trust measurement model based on game theory for social networks. The trust degree criteria are calculated from service reliability, feedback effectiveness, and recommendation validity to obtain a more accurate result. Game theory provides appropriate models and tools for managing multiple interacting entities that try to make decisions and search for a strategic solution that maximizes the utility of each entity by considering trust [15]. In another piece of research, he presented a trust model based on game theory for transport networks without infrastructure. In [16], he presented a model based on attacker and defender security games to identify and deal with attackers and malicious nodes. [17] presents a trusted routing approach based on fuzzy game theory to reduce network attacks in pervasive health monitoring systems. In [18], an energy-efficient trust evaluation scheme is presented, which uses a hierarchical system to reduce the destructive effects of illegitimate sensor nodes and limit the propagation of trust requests throughout the network to reduce energy consumption equipped with reduction of the sensor cluster in the Internet of Things. A model that accumulates indirect trust information among nodes using a trust management system based on game theory that includes a punishment technique to encourage cooperative behaviours has been presented [19]. Huang et al. outline a potential research agenda for advancing the use of game theory and trust to enhance security and utility [20]. The main goal of this research is to provide an overview of existing research on trust and game theory in networks. [21] presents an approach to expanding vehicles' social circles in unreliable networks. To prevent the leakage of sensitive information due to matching user characteristics and the interaction between vehicles, the matching of entities in the SIoV is designed based on privacy protection. The structure of this article is as follows: first, a general definition of this relatively new phenomenon is provided. In the following, the challenges of this type of network are compared to the social Internet of Things. Then, the types of general attacks and threats are examined. Following the current trust approaches and models, the methods of calculating trust in interpretation are discussed. Then the role of fuzzy logic and game theory as an approach to calculate trust is presented, modelled, and then finally, the results of the proposed approach are provided.

Related Works

This section examines trust calculation, general models of trust calculation in social media, trust calculation by fuzzy logic, and game theory in previous research.

FEATURES, CHALLENGES, GENERAL ATTACKS OF TRUST MANAGEMENT

The LDC scheme is an improved version of the ZFTL scheme proposed by Ji et al. [17]. This scheme eliminates the idea of using the Incompressible Data Predictor hardware module in the ZFTL scheme and uses a software module to predict data compression capability [17-18]. The second improvement in this scheme is about garbage collection which proposes a new garbage collection algorithm called compression aware garbage collection. The main idea behind this algorithm is that most data that are detected as incompressible, they have little compression capability. When garbage collection operations in a physical block, if this type of data is valid, then this valid data are compressed in a small amount and written to the boundary between two consecutive pages using the internal fragment space of the physical pages. By compressing this type of data, fewer physical pages are written during garbage collection and thus more free pages remain in a physical block.

Another recently proposed scheme is called EDC [19]. In this scheme, three different types of compression algorithms have been used according to the input data rate in flash memory. If the input data rate is too high, it uses a compression algorithm that has a high compression speed but its compression power is weak. But if the input data rate is low, it uses a compression algorithm that has low speed but high compression power.

Trust in the SIoV has five features: uncertainty, individuality, non-transferability, context-based, and non-cooperativeness, which make it different from traditional social trust [22].

Seven significant management challenges are related to trust in the SIoV. These challenges include the architecture used and how it is implemented, scalability, public reputation, local knowledge, awareness of the context, social communication, trustworthiness, and privacy. These are displayed in the Fig.1 [23].

Fig. 1. Seven major management challenges regarding trust in the SIoV.

The Fig.2 introduces general and trust-related attacks. This list includes common security attacks (that lead to jamming), spoofing attacks, feedback attacks, man-in-the-middle attacks, identity spoofing, domain attacks, and DDoS attacks.

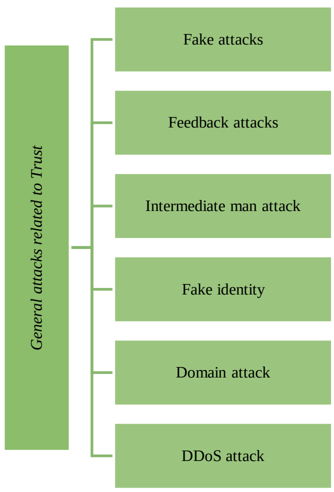

Fig. 2. General trust-related attacks.

Establishing a Trust Model

Approaches to establishing a trust model in vehicular Networks are described in the following:

The first approach: Assigning default credit to each of the new vehicles or leaving them free to share information so that they themselves gain the value of trust. The former scheme is susceptible to masking attacks (meaning that a malicious vehicle with minimal credibility based on its performance disappears from the network and intends to re-enter the network with a new identity, hence its default trust value higher than its original trust, which is obtained from the previous identity).

The second approach: This is for vehicles to share their personal information to gain the trust of other vehicles on the road.

Trust Components

Applying human trust principles to the digital realm is known as computing trust. Marsh et al. claim that projected benefits led to increased cooperation and the use of others' skills through delegation in an open and less protected setting. Research in the area of computing techniques for trust and reliability in online environments has been studied to improve the dependability and effectiveness of online environments [24]. Methods for calculating trust are classified and given in this section. The aim is to identify the research gap in trust computation and then provide a generalization of the presented tree in the social Internet of Transportation [25]. The Fig.3 shows the classification tree based on five design components: trust structure, trust propagation, trust aggregation, trust updating, and trust formation.

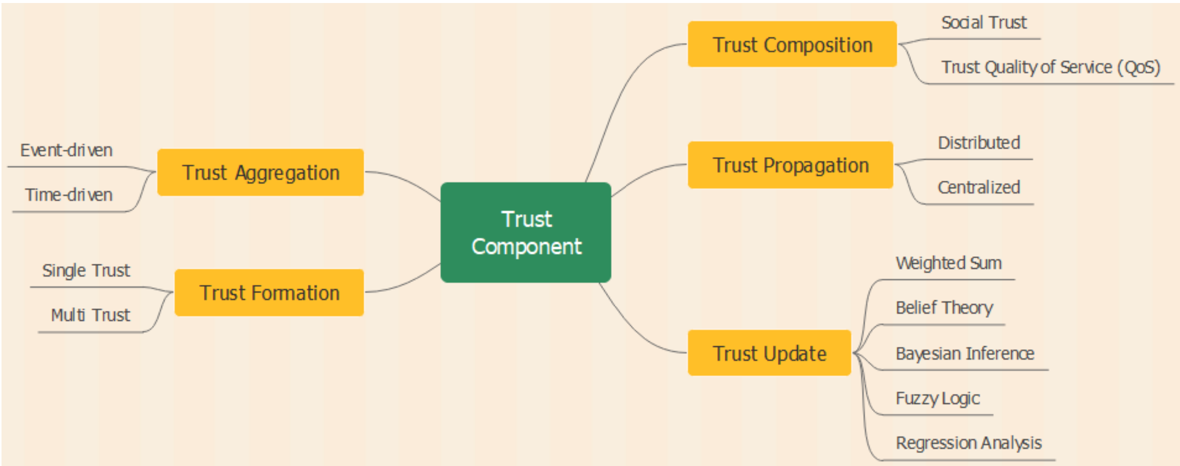

Fig. 3. Classification of different types of trust calculation models [25].

Trust Structure

Trust structure refers to what is considered in trust calculations. Elements of trust include Quality of Service (QoS), trust, and social trust [25]. Quality of Service (QoS) is based on trusting the capability of the IoT device to provide quality services in response to a service request [25]. Trust service quality generally refers to performance and is measured by competence, cooperation, reliability, ability to complete tasks, etc. Nitti and colleagues have used transaction performance to measure the quality of trust service [26]. In [27], metrics such as end-to-end packet transfer rate, energy consumption, and delivery rate are used to measure the quality of service and reliability. Social relationship between IoT device owners provide the basis for social trust, which is assessed using factors including intimacy, honesty, privacy, centrality, and communication. Chen et al. have used friendship, social connections, and community of interest to evaluate a voter [28]. Chen et al. have measured social trust by the criteria of connection, intimacy, honesty, and unselfishness [29]. Social trust is pervasive in social IoT networks. IoT devices should be assessed based on social trust (i.e., organizational commitment and goodwill in performing a service) and service quality (a device's capacity to execute the service). Furthermore, when using a recommendation, an IoT device should trust connected social devices (from their owners) rather than unrelated devices.

Trust Propagation

The term "trust propagation" describes how peers spread proof of trust. The two primary methods for propagating trust are distributed and centralized [25]. Distributed trust propagation refers to IoT devices that spontaneously and without a centralized entity propagate trust observations to other IoT devices they encounter or communicate with [28]. This type of trust promotion is beneficial in cases in which it is difficult to configure or access a centralized entity in IoT environments with infrastructure-less networks (such as wireless networks without mobile infrastructure or a wireless sensor network). Chen et al. have proposed an approach to distribute trust between social IoT systems so that each node of the network maintains a data table of information collected according to the activities of its neighboring nodes [27]. Guo et al. argue that distributing centralized trust requires a centralized system, such as a physical cloud or a virtualized trust system operated by IoT nodes [25].

Nitti et al. have presented a structure based on the distributed hash table to preserve trust information related to each node [26]. Saeed and associates have also presented a centralized system for trust management to keep track of the IoT entities that may be trusted and choose those that can respond to service requests [30].

Trust Aggregation

Aggregation of trust information refers to the collection of trust evidence gathered through individual observations of each node or provided from peer feedback. Trust aggregation methods have been mainly studied by Zhusang et al., including weighted sum components, belief theory, Bayesian inference (with belief reduction), fuzzy logic, and regression analysis [31].

Trust Update

Trust updating generally deals with the category of trust updating and includes two approaches: event-based and time-based [25]. Event-based trust updating: In the event-based approach, all trust data in a node is updated after a transaction or event [25]. After providing a service, it is obtained from feedback about the service quality that is sent to the cloud trust manager or recorded in the node's memory for collecting trust. A recommendation can also be sent upon request in feedback-based environments. This way, nodes can communicate and seek advice from other nodes [32]. Time-based trust updating: In the time-based approach, evidence (individual observations or recommendations) is collected periodically, and trust is updated by one of the cumulative trust methods [33]. If no evidence is collected, the old trust information expires, because recent information is more reliable than past information. According to the application's specific needs over time, the expiration function is used by the parameters of the degree of trust weakening [33].

Trust Formation

Establishing trust refers to the overall formation of trust among several features. In general, trust formation has two aspects: integrated trust and multiple trust [25]. Establishing integrated trust refers to the fact that only one trust index is considered in the trust protocol [28]. The creation of multiple trust shows shared belief and multidimensional trust. Therefore, multiple features of trust should be considered in creating trust [30].

General Models of Trust

Mohammadi et al. in [35], the degree of trust according to three criteria and from three aspects, service reliability, effective feedback, and recommendation validity, was used to calculate trust. In addition, to solve the problem of liberalization, a punitive mechanism based on game theory is used for specific trust and global trust and the problem of free riders (so-called people who try to use other people's network resources without using their own resources in the exchange). The main goal is to provide an electronic trust measurement model that can strengthen social network services (such as feedback control, suggestions, and strategy selection). To solve these problems and in order to be more accurate in the degree of trust of a node, three new evaluation factors - reliability, feedback, and validity - have been used. To solve the free-riding problem, Wang et al. have implemented penalties for the specific and overall trust that operates differently from conventional statistical techniques. The proposed punishment mechanism consists of evolutionary game theory, which has greater flexibility and effectiveness [36]. Smaldon et al. used the term social transportation network for the first time in their article about peak traffic in such a way that they used the vehicle network in human society and applications such as entertainment, convenience, and emergency messages [37]. Hu et al. also introduced a social driving system that increases driver awareness about fuel economy [38]. Guinard et al. discussed how websites could share performance interfaces using human social network infrastructures such as Facebook, LinkedIn, and Twitter [39]. Holmquist and colleagues have investigated how to establish quality wireless communication between intelligent objects [40]. Recently, there has been a growing interest in creating a social Internet of Things [41-42]. The Social Internet of Things focuses on creating and exploiting social relationship (e.g., parent object relationship, neighborhood object relationship, etc.) among objects instead of their owners. In research on the social Internet of Things, it has been found that the structure of human social networks is unsuitable for different objects due to their unique nature. It shows the types of social network structures: a) a car-based static home social network, b) fully dynamic social network, and c) dynamic car social network visit [25]. Table 1 also compares the approaches and methods of trust calculation in wireless networks without infrastructure according to the architecture, the criteria, the approach, the field of activity, and the proposed method.

Table 1

Comparison of approaches and methods for calculating trust in wireless networks without infrastructure.

Proposed Model	Area	Approach	Criteria	Architecture
A fuzzy model for computation of trust in FANET[43]	FANET	Fuzzy Classification	QOS Social Parameters	Decentralized
An Underwater Wireless Sensor Networks Trust Cloud Model[44]	Underwater WSN	Cloud Theory Fuzzy Logic	Energy, Honesty	Centralized
A rating system for Trust Management in SIoV[45]	SIOV	Rater-Based	Popularity, Integrality, Indelibility	Decentralized
Trust model for secure group leader-based communications in VANET [16]	VANET	Hybrid Trust Model (HTM)	Honesty Cooperativeness	Decentralized
Trust-Based Cooperative Game Model for Secure Collaboration in the Internet of Vehicles[46]	IoV	Bayesian Inference Model & Hedonic Cooperative Game Model	Trustworthiness Legitimacy Cooperativeness	Decentralized
RpR: A Trust Computation Model for Social Internet of Things[34]	SIOV	Reputations Based Trust Computational Model	Trustworthiness popularity	Decentralized

1. The Framework of The Proposed Method

In the following, the framework components of the proposed method are discussed in order.

Net Present Value in Trust

Current net worth is one criteria for measuring the economic value of projects, which includes concepts such as the value and social value of projects. In this research, a map of this current net worth has been made in social networks, especially the SIoV. The expression of this concept is as follows and is obtained from Eq. 1 [47]:

$$NPV = C_0 + \sum_{t=1}^{\infty} \beta^t \cdot C_t \qquad \text{Eq (1)}$$

In economic projects, C_0 represents the project's cash flow in the zero period, and its value is usually negative and indicates an initial investment. In this research, C_0 indicates the amount of initial trust attributed to the social entity. Also, C_t is the cash flow resulting from project investment in period t, and $\beta^t$is the discount factor for period t obtained from the following relationship. Therefore, C_t is the level of trust gained in period t; similarly, Eq. 2 represents$\beta^t$and the factor of reducing the level of trust in the period [47].

$$\beta^t = \frac{1}{(1+r)^t} \qquad \text{Eq (2)}$$

Fuzzy Net Present Value in Trust

A multivalued logic uses approximate reasoning instead of fixed and exact reasoning. Unlike traditional binary arrays, fuzzy logic variables may have real values ranging from 0 to 1. The issue of partial truth, where the truth value can range from absolutely true to false, has been handled by fuzzy logic. Specific membership functions may also handle these degrees when linguistic variables are present. Fuzzy net present value Although definite predictions are usually used in calculating net present value in the number of investment calculations and the resulting cash flow, these predictions are always faced with ambiguity and uncertainty. This is the same as trust calculations that have a human nature (even calculations of network and social entities). Therefore, fuzzy theory is used to calculate the net present value to consider this uncertainty. Credibility and trust are fuzzy measures, with membership functions showing the degree of trust. For example, confidence values in the range (1.25 and -1.25) indicate very low confidence (0, 2.5) low confidence (1.25, 3.75) moderate confidence, (2.5, 5) high confidence, (3.75, 6.25) high confidence. Hence, a node with a credit value of 0.25 has a very low trust (a membership function) of 75% and a low trust (of other membership functions) of 25%. Fuzzy logic provides rules for fuzzy reasoning by fuzzy criteria. Chen et al. in [48] used the fuzzy membership function according to the number of positive and negative experiences and the criterion of uncertainty to calculate trust. Eq. 3 expresses the fuzzy net present value, and Eq. 4 expresses the discount factor for period t [48].

$$N\tilde{P}V = \tilde{C}_0 + \sum_{t=1}^{\infty} \beta^t \cdot \tilde{C}_t \qquad \text{Eq (3)}$$

$$\beta^t = \frac{1}{(1+r)^t} \qquad \text{Eq (4)}$$

Game Theory and Trust

Game theory is a branch of applied mathematics used in many fields of science, especially computer engineering. Game theory tries to get a behavior through mathematics in a strategic situation, or game, in which the choice's success depends on others' choices [49]. Using scenario design and analysis, game theory tries to predict the behavior and decision results of beings with the right to choose when interacting with each other. Each game consists of a set of players, a set of moves or strategies, and a specific outcome for each combination of strategies. The theory of games tries to model the behavior governing a strategic situation (conflict of interests) [50]. This situation arises when a person's success depends on the strategies others choose. The ultimate goal of this knowledge is to find the optimal strategy for players [51].

International Journal of Multiphysics
Volume 18, No. 4, 2024
ISSN: 1750-9548

Every game has three main components:

1. Players; People who are in charge of making decisions in the game [52].
2. Strategies; Tell the characteristics of each decision in each specific situation [52].
3. Rewards; Win or lose in cases where each actor follows a particular strategy [52].

Methods of displaying games:

Matrix: modeling the game regardless of time, and players choose their strategy simultaneously. This type of display is often used to display static games. In game theory, this type of display is also called normal display [53].

Tree graph: In game modeling, time is considered a changeable component in the time interval, and the decision of each actor is considered in each time interval. This type of display is often used to display dynamic games. In game theory, this type of show is also called an extended show [53].

Cooperative games and non-cooperative games:

Cooperative games are such that players are committed to adopting a specific strategy through negotiation and agreement between players [55]. Non-cooperative games refer to games in which players decide to maximize their profits by their strategy [55].

Cooperative games and non-cooperative games:

Cooperative games are such that players are committed to adopting a specific strategy through negotiation and agreement between players [54]. Non-cooperative games refer to games in which players decide to maximize their profits by their strategy [54].

Shapley Value

For an N-player game with cooperation, Shapley has calculated the average income of each player from alliances. In the sense that this concept determines the received value $(S * i)$ of the i-th player. If the i-th player joins coalition C,his final productivity, to this coalition is defined from Eq. 5 and as the following [55]:

$$\{v(C) - v(C - (i))\} \qquad \text{Eq (5)}$$

Assuming that the coalitions are generally formed from one person to two and to N people, and any order of joining the coalitions is possible, S_i^* belonging to the i-th player will represent his final average productivity in the game, which is calculated by Eq. 6 [56].

$$S_i^* = \sum_{\{\substack{C \subset N \\ i \in C}} \frac{(k-1)!(N-k)!}{N!} \{V(C) - V(C - (i))\} \qquad \text{Eq (6)}$$

Such that$N$is the total number of players, K is the number of players in the coalition, and $((K-1)!(N-K)!)/N!$is the probability of each coalition.

From the sum of calculations, it is obtained for each possible coalition of the i-th participant. The Shapley value of $(S_i{}^*)$ can determine the strength of the i-th player in his sensitivity and influence to win a coalition. This power depends on increasing the productivity of a coalition from the i-th player joining that coalition [55].

Fuzzy Shapley Value

In this study, the desirability of each strategy is obtained through a fuzzy calculation for each strategy. Therefore, for each combination of strategies, four benefits $\widetilde{U}_{IP}$, $\widetilde{U}_{IC}$, $\widetilde{U}_{HP}$, $\widetilde{U}_{HC}$ are determined for players IP, IC, HP, HC; Then, the degree of desirability of binary, triple and quadruple alliances is determined for each strategy combination.

$$\widetilde{U}_{IC,IP}(HC, HP, IC, IP) = \widetilde{U}_{HC}(HC, HP, IC, IP) + \widetilde{U}_{HP}(HC, HP, IC, IP) \text{ Eq (7)}$$

The value of the characteristic function $\tilde{V}(C)$ of the coalition Cin the normal (two-dimensional) form, according to the view of Van Newman and Morgenstern, has the characteristics of a saddle point. The row's maximum-minimum and the column's minimum-maximum coincide with each other at a saddle point because the members in the row try to maximize the minimum of their utility, and the non-members in the column try to minimize the maximum loss. Although the cooperators themselves may have a positive income anyway, a lower income for the cooperators can lead to a higher income for them [55].

In general, the characteristics of a point of a saddle point for a game in normal (and two-dimensional) form can be obtained from the solution of a $L-P$(for the cooperators in the row) [55].

$\tilde{V}(C)$defined for a non-zero two-dimensional game (consisting of Nplayers) provides$V(\emptyset)=0$ property, includes "beyond collectivity," and is calculated through Eq. 8. Accordingly, if $\tilde{C}_{ij}$ represents the coalition's desirability from the j-th column and i-th row of the coalition matrix (coalition C). The i-th row represents a combination of coalition strategies, and the j-th column represents a combination of non-coalition strategies; thus, $\tilde{V}(C)$ is obtained from the following fuzzy$L-P$ solution [55].

$$\begin{aligned}&\tilde{V}(C)=MAX{:}\,Z\\&Z\le\textstyle\sum_i p_i\,.\,\tilde{C}_{i,j}\rightarrow\forall j\\&s.t{:}\\&\quad\textstyle\sum_i p_i=1\\&\quad p_i\ge 0, Z{:}\,free\end{aligned}\qquad \text{Eq (8)}$$

P_i specifies the probability of selection (from the combinations of strategies in the i-th row) for the allies. To obtain the characteristic function of different coalitions, linear programming (Eq. 4) is written based on the normal matrix of the coalition's utility$C$, and the value$\tilde{V}(C)$ of each coalition is also calculated by solving the model by Eq. 9-1, Eq. 9-2 and Eq. 9-3 is obtained.

It assumes that $C_{ij}=(C_{ij1},C_{ij2},C_{ij3})$is three deterministic linear programming models and is written as follows. Therefore, the value of $\tilde{V}(C)=V_1(C),V_2(C),V_3(C)$ is obtained [55].

$$\begin{aligned}&V_1(C)=MAX{:}\,Z\\&s.t{:}\\&\quad Z\le\textstyle\sum_i p_i\,.\,C_{ij1}\rightarrow\forall j\\&\quad p_i\ge 0\\&\quad Z{:}\,free\end{aligned}\qquad \text{Eq (9-1)}$$

$$\begin{aligned}&V_2(C)=MAX{:}\,Z\\&s.t{:}\\&\quad Z\le\textstyle\sum_i p_i\,.\,C_{ij2}\rightarrow\forall j\\&\quad p_i\ge 0\\&\quad Z{:}\,free\end{aligned}\qquad \text{Eq (9-2)}$$

$$\begin{aligned}&V_3(C)=MAX{:}\,Z\\&s.t{:}\\&\quad Z\le\textstyle\sum_i p_i\,.\,C_{ij3}\rightarrow\forall j\\&\quad p_i\ge 0\\&\quad Z{:}\,free\end{aligned}\qquad \text{Eq (9-3)}$$

Finally, the value of the fuzzy Shapley value is calculated from Eq. 10 for each player, and the values of the fuzzy Shapley value are ranked [56].

$$\tilde{S}_i^*=\sum_{\left\{\substack{C\subset N\\ i\,\in\, C}\right.}\frac{(k-1)!(N-k)!}{N!}\{\tilde{V}(C)-\tilde{V}(C-(i))\}\qquad \text{Eq (10)}$$

In [56], the fuzzy Shapley value has been calculated through credit theory with fuzzy receipts. In [57] and [58], the cooperation between the players is considered in a fuzzy form, and the Shapley value is calculated.

Examining the steps and methodology of the proposed framework

In the first stage, the criteria of honesty, intimacy, communication, and privacy are the main criteria of the IHPC matrix. Then the analysis of the IHPC matrix is performed at the simulator level. Next, by considering and identifying the connections of these criteria, they are placed in a two-by-two matrix, and various possible strategies are deduced.

In the second step, different combinations are obtained from implementing the strategies of each facet of the IHPC matrix. In the third step, each strategy's fuzzy net present value is calculated according to the combination of the strategy being implemented. Each strategy requires certain activities to calculate trust, and each of these activities involves a cost, but over time, this is the Cost. According to the success rate of the strategy in the proposed method, the trust calculation process will be more accessible, and the costs will be reduced. In this time interval section, the simulation execution time for each strategy combination is considered. Comparing the obtained net present values in the degree of utility of different strategies is considered the ratio of the present net trust value to the initial trust amount. This is calculated by Eq. 11 [58].

$$\widetilde{U} = \frac{N\tilde{P}V}{\tilde{C}_o} \qquad \text{Eq (11)}$$

Also, there may be joint operations in the combination of strategy implementation, which reduce the cost of trust calculations of strategies. For example, by simultaneously implementing two or more strategies, the success rate of strategies increases. Hence, confidence values in implementing one strategy combination will be different from another.

In the fourth step, the desirability matrix of the combination of strategies is obtained.

In the fifth step, the specification function of each coalition is calculated with the Van Neumann-Mungstern approach to solving Eq. 9.

In the sixth step, the fuzzy Shapley value of each player is obtained from Eq .10, and they are ranked by fuzzy ranking.

In the seventh step, according to the Shapley value obtained for the players, which indicates the order of importance of the players in the strategy combination, the appropriate combination is selected for execution.

In the final stage, if the strengths and weaknesses are identified with a new threat and opportunity, the process repeats itself and updates its proposed method to adapt to the new environmental situation; otherwise, the process ends.

2. Levels of the Proposed Framework

The proposed framework consists of four levels, as shown in the Fig. 4. The first level (goal) is choosing the best strategy. The second level includes trust factors (honesty, intimacy, communication, privacy). The third level of subfactors (H1, H2..., I1, I2..., p1, p2..., C1C2...). The fourth level includes four strategies (HC, HP, IC, IP).

In the proposed framework, it is assumed that trust factors are in mutual opposition. There is also a relationship between the two factors of honesty and sincerity.

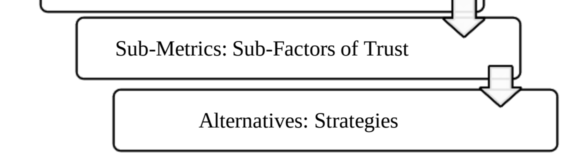

Fig. 4. Structure of the proposed method.

Flowchart of the Proposed Framework

This section presents the case study and the steps of the proposed method, then shows its conceptual flowchart, as shown in the Fig 5.

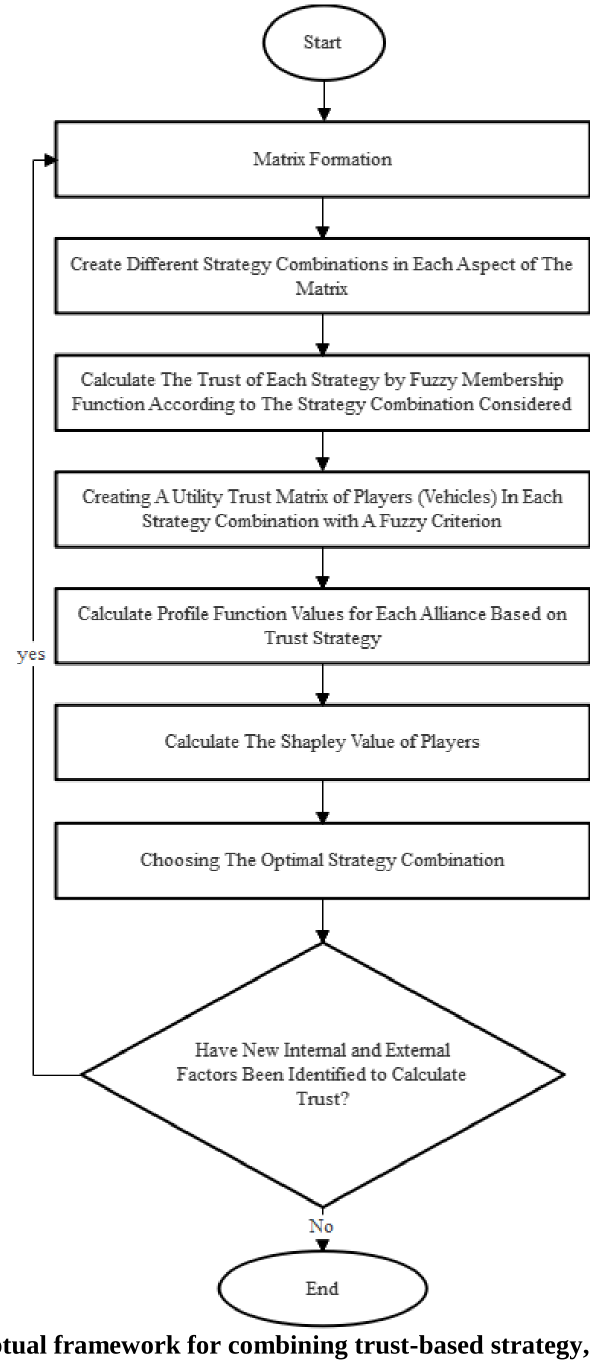

Fig. 5. Conceptual framework for combining trust-based strategy, Shapley value.

Case Study and Examination of The Steps of The Proposed Method

The proposed method consists of the following stages. In the first stage, the strategies that lead to trust in the SIoV is considered in the form of a two-by-two matrix (Fig. 6). The second stage shows the simulation platform as well as different combinations of strategies in each facet of the obtained matrix. Fig. 7 shows the various combinations of strategies obtained. Third level: Dependencies between IHPC matrix strategies are investigated. In the fourth stage, the utility matrix of strategy combination is obtained. In the fifth stage, the characteristic function of each coalition is obtained from Eq. 4 with the Van Neumann-Mungstern approach. According to the van Neumann-

Mungstern L-P approach obtained from Eq. 4 for single, double and triple, and quadruple coalitions of players, the values of the characteristics of each coalition were obtained in a fuzzy manner. Table 2 shows the relationships between the strategies of the IHPC matrix, and then the fuzzy preferences of the players in each strategy combination are shown in Table 3. In Fig. 8, the cumulative column chart of the fuzzy preferences of the players in each strategy combination is also shown. In Table 4, the characteristic function values for each coalition are shown. For a better display in Fig. 9, box and line diagrams are also used to check the proximity of the fuzzy values of the characteristic function for each coalition. In Fig. 10, the cluster column chart compares the values in the categories of the characteristic function values for each coalition.

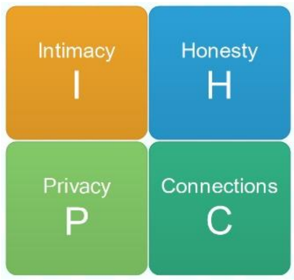

Fig. 6. Trust Matrix.

3. Findings and Results of the Proposed Framework

According to the simulation, an IHPC matrix was obtained; Then, the network entities randomly determined the effect of one strategy on another strategy, and this effect was specified in the corresponding table with a star symbol. Finally, the table of dependence between the strategy of different aspects of the IHPC matrix was formed in Table 1. According to the strategy's existing dependencies, the entities' trust level was determined during the simulation period. Then, the estimated values of trust were converted into fuzzy triangular numbers. Their fuzzy net present value was obtained through Eq. 3. The ratio of net current value to initial trust values for each strategy in each strategy combination was obtained through Eq. 11. The desirability of each player was considered in the strategy combination in the structure of cooperative games. Table 2 shows the fuzzy benefits obtained for the players in each strategy combination.

According to Van Neumann and Mungstern's approach and the solution of L-Ps obtained from Eq. 9 for single, double, triple, and quadruple coalitions of players, the characteristic function values for each coalition were obtained in a fuzzy manner. The specification function values for each coalition are listed in Table 3.

By using the Eq. 10, the fuzzy value corresponding to each player is calculated, and the obtained fuzzy values are ranked. The combination of IC > HC > HP > IP in the ranking of calculated Shapley values is obtained for the players. This order shows the importance of the players and their sensitivity and influence in winning a coalition. Therefore, the decision to choose a strategy is made between the strongest and weakest players.

	Privacy(P)	Connections(C)
Honesty(H)	Strategy: HP 1.Expectations 2.Reliability	Strategy: HC 1.Evaluation of Objectives 2.Social Equations
Intimacy(I)	Strategy: IP 1.Environment 2.Public Reputation	Strategy: IC 1.Popularity 2.Local Knowledge

Fig. 7. The overall structure of the trust matrix.

Table 2

International Journal of Multiphysics
Volume 18, No. 4, 2024
ISSN: 1750-9548

Coregulations between IHPC matrix strategies.

	IC	IC	IP	IP	HC	HC	HP	HP
HP1		☑	☑		☑		☑	
HP2	☑			☑		☑		☑
HC1	☑			☑			☑	
HC2		☑	☑					☑
IP1	☑	☑				☑	☑	
IP2		☑						☑
IC1			☑	☑	☑			☑
IC2				☑	☑	☑	☑	

Table 3

Fuzzy desirability of players in each strategy combination (desirability matrix)

Desirability matrix				
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)	(-0.18,0.19,1.16)	(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)	(-0.28,0.03,0.69)	(-0.02,0.57,0.66)
HC2, HP1, IC2, IP1	(-0.01,0.38,0. 48)	(-0.01,0.38,0. 48)	(-0.01,0.38,0. 48)	(0.022, -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, IP1	(0.16, 0.49,0.99)	(-0.13, 0.49,1.36)	(-0.38, 0.99,1.32)	(0.14, 0.49,0.99)

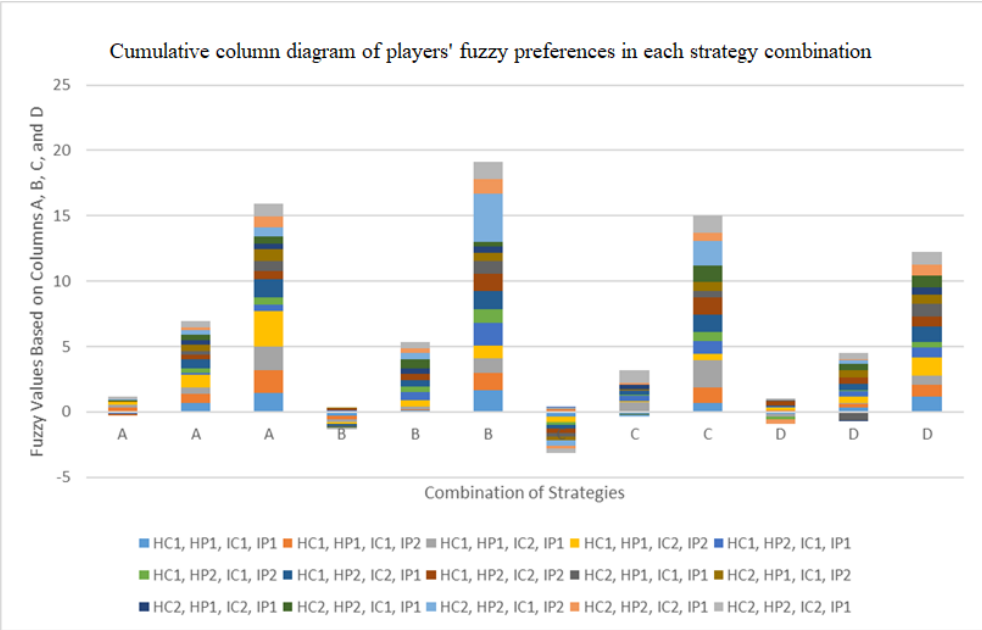

Fig. 8. Cumulative column diagram of players' fuzzy preferences in each strategy combination. Here is a cumulative column chart to compare the overall fuzzy values that are used in four columns A, B, C, and D. It shows the fuzzy changes of the values over time, based on the combination of strategies.

Table 4

Values of specification function for each coalition

Coalition(c)	Ṽ(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	)0.9,0.1, 0.63(-
HC-HP	(0.24,0.66,2.03)
HC-IC	(-0.10,1.3,4.88)
IP- HP	(-0.01,0.8,2.11)
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)
HC-HP- IC- IP	(-0.06,1.62,6.36)

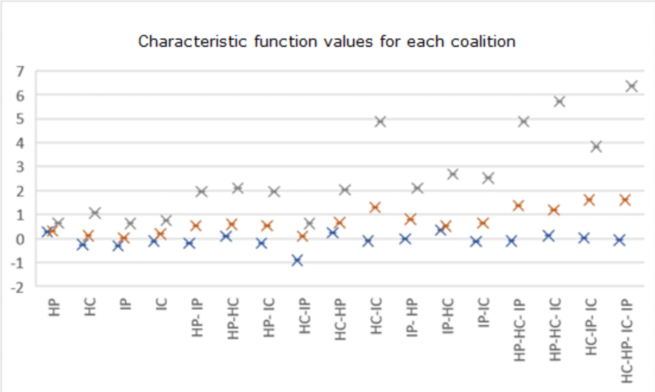

Fig. 9. Here, box and line plots are used to examine the proximity of the fuzzy values of the characteristic function for each coalition. The reason to use this chart is because of its high readability and ease of use, since it can summarize data from multiple sources and display the results in one chart. Box and line charts enable data comparison from different categories for more accessible and effective decision-making.

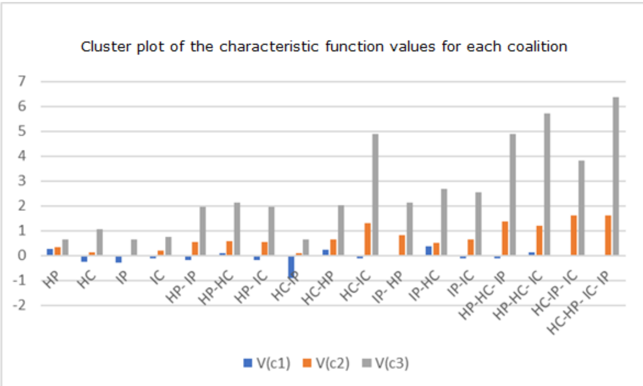

Fig. 10. A cluster column chart is used to compare the values in the categories of values of the characteristic function for each coalition. The reason for using this diagram is that the order of the specification function value categories is not essential for each coalition, but the comparison of the fuzzy values of the specification function is necessary for each coalition.

In the sixth step, using the Eq. 10, the fuzzy value for each player is calculated. The obtained fuzzy values are ranked, and the combination of IC > HC > HP > IP in the ranking of calculated Shapley values is obtained for the players. This order indicates the order of importance of players in their sensitivity and influence to win a coalition is shown in Table 5. Therefore, the decision to choose a strategy is made between the strongest and weakest players. In Fig. 11, the cumulative column chart shows the fuzzy Shapley value of the players with respect to the selected players. It indicates the order of importance of the players in their sensitivity and influence to win a coalition. And finally, in Fig. 12 is a cluster column chart to compare the players' fuzzy Shapley value values for the selected players. It shows the importance of the players in their sensitivity and influence to win a coalition. The reason for using this chart is that the order of players and the value of fuzzy Shapley is essential, and it shows the decision process for choosing a strategy from the strongest player to the weakest player.

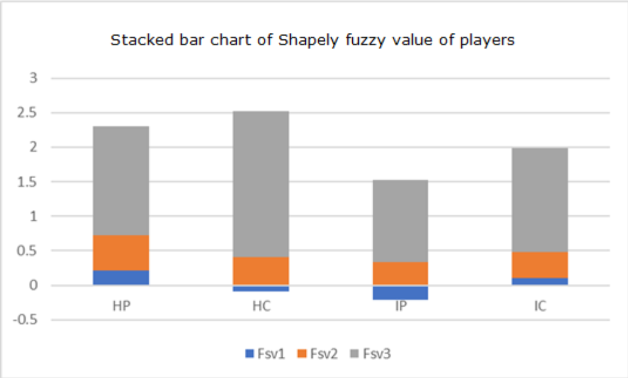

Fig. 11. A stacked column chart showing the players' fuzzy Shapley value with respect to the selected players and showing the order of players' importance in their sensitivity and influence in winning a coalition.

Table 5

Player's fuzzy shapley values

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

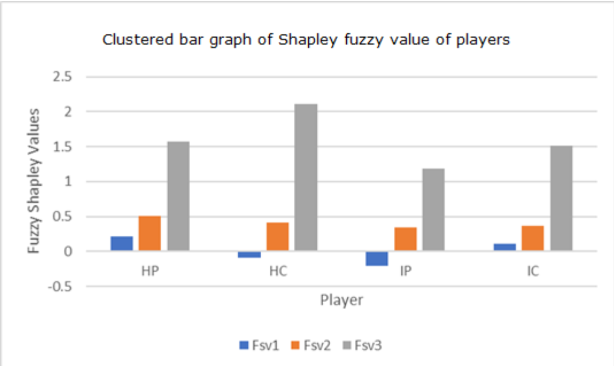

Fig. 12. Clustered column chart to compare the fuzzy Shapley value values of the players with respect to the selected players. It shows the order of importance of the players in their sensitivity and influence in winning a coalition. The reason for using this chart is that the order of players and the fuzzy Shapley values are essential, and it shows the decision process for choosing a strategy from the strongest player to the weakest player.

In the seventh step, according to the Shapley value obtained for the players, which indicates the order of importance of the players in using the strategy combination, the appropriate combination is selected for execution. In the final stage, if other trust factors are identified, the process is repeated again; otherwise, the process ends.

4. Simulation Environment

This section describes the simulation platforms used in the evaluations performed on the proposed method. After that, we will give the simulation results of the proposed plan. The simulation platform is created from a combination of OMNet++, SUMO, and Veins. The OMNet++ tool is used as a network simulator, and the Sumo tool as a traffic simulator. These two tools communicate with each other by means of Veins. In the following, we will describe each of these simulators separately.

Metrics Table

SUMO

SUMO is one of the most well-known simulated platforms that has been developed as open source. There is no limit to its use and development. SUMO simulates the structure of a traffic network, including streets and their characteristics. It also specifies the type of vehicles, routes, and other traffic characteristics. Each traffic network is considered a series of two-dimensional points connected by an oriented edge. It is necessary to consider that the traffic flow network is assumed to be flat and two-dimensional, and its three-dimensional state is also mapped to the two-dimensional model with simple techniques. Creating this traffic network is possible in two ways. The first method is to search for a desired location map on the OpenStreetMap site and extract the map in osm format with the desired magnification. After that, we create the necessary files for OMNET++ with the commands available in Sumo. In the second method, the map is created manually. The desired files must also be created manually. In Sumo, automobiles have various parameters, such as the length of the vehicle, acceleration, brake, and maximum speed. In addition, it requires a parameter called sigma, which introduces some random behaviors and is based on vehicle type and case. Setting this parameter to 0.0 presents a deterministic vehicle (no random behaviors). After determining the characteristics of each vehicle, we define a path that includes two edges. The reason for using two edges is that the vehicle's position is determined based on its front position. Ultimately, we write the vehicle description and save the file with the extension rou.xml. In the next phase, we link all the files we created and store them all in Sumo.cfg configuration file.

OMNET++

This tool is free and only available for academic and scientific work. It is used to simulate network events and is based on discrete event architecture and piece modules. This functionality makes the network design, troubleshooting, and rebuilding processes incredibly simple. This simulator is used in various applications such as network traffic modeling, protocol modeling, queuing network modeling, and evaluation of how to implement complex software systems [60].

VEINS

For continuous communication between the traffic simulator, i.e., Sumo, and the network simulator, i.e., OMNET++, the Veins tool is used. In fact, the proper combination of communication and motion models during the simulation's execution reduces the simulation's complexity. Veins enables a two-way compound simulation. The two-way combination allows the network simulation to directly control the road traffic simulation, thereby simulating the impact of the vehicular case network communications on the road traffic. Traffic simulation provides the necessary information for the network simulator. In [61], he described the need for a two-way combination of accurate motion models and simulation tools to evaluate automotive case network protocols. An evaluation and history of motion models used in the simulation of automotive ad hoc network protocols are presented in [62]. This paper introduces four types of motion models: 1) random node motion, 2) real-world motion tracking, 3) intelligent motion tracking 4) two-way hybrid simulation. In addition, Veins includes the 802.11P physical and MAC layers, through which it handles periodic WAVE messages and multi-channel processing and switching between channels. Veins is basically based on the Maxim model, and it calculates the interference values and the signal-to-noise ratio. Maxim is a modeling framework based on OMNET++ for wireless and mobile networks. Fig. 13 shows the relationship between these three tools [63]. In Fig. 14, you can see the map used in the simulated scenario, and in Fig. 15, an enlarged part of the map used in the simulation is displayed.

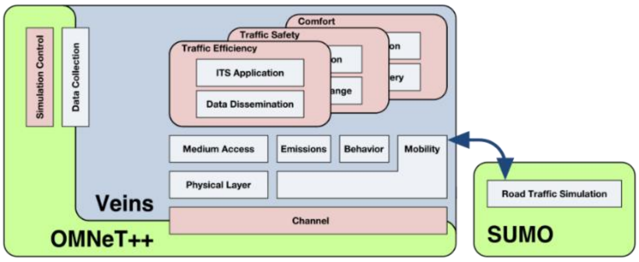

Fig. 13. The substrate used in the simulation [62].

Fig. 14. Used scenario created in Veins.

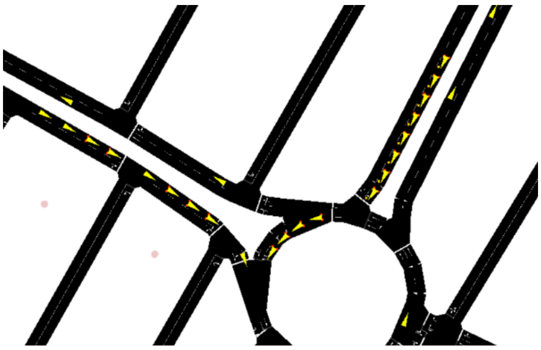

Fig. 15. Enlargement of a part of the map used in the simulation.

5. Conclusion

This research sought to provide a reliable framework consistent with fuzzy logic and game theory. The proposed method consisted of four levels, the first level (goal), which is the choice of the best strategy, and the second level is trust factors (honesty, intimacy, communication, privacy). The third level of sub-factors is H1, H2..., I1, I2..., p1, p2..., C1C2... and the fourth level is the four strategies (HC, HP, IC, IP). In the proposed method, it is assumed that trust factors are in mutual opposition. There is also a relationship between the two factors of honesty and sincerity. Considering the conditions and theory of cooperative games, the Shapley fuzzy value of each player, which is the coalition power of each facet in strategic cooperation between faces, is determined. The best strategy is chosen by determining the importance of each aspect based on the ability of the players in the coalition.

References

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. Rahim *et al.*, “Vehicular Social Networks: A survey,” *Pervasive and Mobile Computing*, vol. 43, pp. 96–113, 2018, doi: 10.1016/j.pmcj.2017.12.004.
3. K. M. Alam, M. Saini, and A. el Saddik, “Toward social internet of vehicles: Concept, architecture, and applications,” *IEEE Access*, vol. 3, no. c, pp. 343–357, 2015, doi: 10.1109/ACCESS.2015.2416657.
4. K. M. Alam, M. Saini, and A. el Saddik, “Toward social internet of vehicles: Concept, architecture, and applications,” *IEEE Access*, vol. 3, no. c, pp. 343–357, 2015, doi: 10.1109/ACCESS.2015.2416657.
5. Siddiqa *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.
6. M. Hossain, R. Hasan, and S. Zawoad, “Trust-IoV: A trustworthy forensic investigation framework for the internet of vehicles (IoV),” *Proceedings - 2017 IEEE 2nd International Congress on Internet of Things, ICIOT 2017*, pp. 25–32, 2017, doi: 10.1109/IEEE.ICIOT.2017.13.
7. C. A. Kerrache *et al.*, “TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles,” *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 5870–5877, 2019, doi: 10.1109/JIOT.2018.2880332.
8. J. Golbeck, “Computing with trust: Definition, properties, and algorithms,” *2006 Securecomm and Workshops*, 2006, doi: 10.1109/SECCOMW.2006.359579.
9. J. Golbeck *et al.*, “RoadSpeak,” *2006 Securecomm and Workshops*, vol. 3, pp. 139–149, 2008, doi: 10.1109/BlackSeaCom.2014.6849025.
10. T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, “Privacy Management in Social Internet of Vehicles: Review, Challenges and Blockchain Based Solutions,” *IEEE Access*, vol. 7, pp. 79694–79713, 2019, doi: 10.1109/ACCESS.2019.2922236.
11. 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, Sep. 2021, doi: 10.3390/electronics10182223.
12. J. M. Chen, T. T. Li, and J. Panneerselvam, “TMEC: A Trust Management Based on Evidence Combination on Attack-Resistant and Collaborative Internet of Vehicles,” *IEEE Access*, vol. 7, pp. 148913–148922, 2019, doi: 10.1109/ACCESS.2018.2876153.
13. X. Wang, P. Zhang, Y. Du, and M. Qi, “Trust Routing Protocol Based on Cloud-Based Fuzzy Petri Net and Trust Entropy for Mobile Ad hoc Network,” *IEEE Access*, vol. 8, pp. 47675–47693, 2020, doi: 10.1109/ACCESS.2020.2978143.
14. Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong, and Q. Han, “A game theory-based trust measurement model for social networks,” *Computational Social Networks*, vol. 3, no. 1, 2016, doi: 10.1186/s40649-016-0027-x.
15. J. Antoniou, “Using Game Theory to Motivate Trust in Ad Hoc Vehicular Networks,” pp. 61–84, 2020, doi: 10.1007/978-3-030-16844-5_4.
16. M. M. Mehdi, I. Raza, and S. A. Hussain, “A game theory based trust model for Vehicular Ad hoc Networks (VANETs),” *Computer Networks*, vol. 121, pp. 152–172, 2017, doi: 10.1016/j.comnet.2017.04.024.
17. K. Geetha and P. Thangaraj, “FGT2- ABR: Fuzzy game theory trust associativity based routing to mitigate network attacks in pervasive health monitoring systems,” *Journal of Pure and Applied Microbiology*, vol. 9, no. Special Edition, pp. 161–168, 2015.
18. R. Rani, S. Kumar, and U. Dohare, “Trust Evaluation for Light Weight Security in Sensor Enabled Internet of Things: Game Theory Oriented Approach,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8421–8432, 2019, doi: 10.1109/JIOT.2019.2917763.
19. H. J. Li, Q. Wang, S. Liu, and J. Hu, “Exploring the trust management mechanism in self-organizing complex network based on game theory,” *Physica A: Statistical Mechanics and its Applications*, vol. 542, 2020, doi: 10.1016/j.physa.2019.123514.
20. L. Huang, G. Jia, W. Fang, W. Chen, and W. Zhang, “Towards security joint trust and game theory for maximizing utility: Challenges and countermeasures,” *Sensors (Switzerland)*, vol. 20, no. 1, pp. 1–15, 2020, doi: 10.3390/s20010221.
21. C. Lai, Y. Du, Q. Guo, and D. Zheng, “A trust-based privacy-preserving friend matching scheme in social Internet of Vehicles,” *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 2011–2025, Apr. 2021, doi: 10.1007/s12083-021-01140-3.
22. H. Vahdat-Nejad *et al.*, “Social internet of vehicles for smart cities,” *IEEE Access*, vol. 7, no. 4, pp. 1–6, 2019, doi: 10.3390/jsan5010003.

23. R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, “Trust management in social Internet of vehicles: Factors, challenges, blockchain, and fog solutions,” *International Journal of Distributed Sensor Networks*, vol. 15, no. 1, 2019, doi: 10.1177/1550147719825820.
24. “The Connected Automobile Nears Critical Mass (2015) Trends Magazine. Apr2015, Issue 144, 31-35.”
25. J. Guo, I. R. Chen, and J. J. P. Tsai, “A survey of trust computation models for service management in internet of things systems,” *Computer Communications*, vol. 97, pp. 1–14, 2017, doi: 10.1016/j.comcom.2016.10.012.
26. M. Nitti, R. Girau, and L. Atzori, “Trustworthiness management in the social internet of things,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1253–1266, 2014, doi: 10.1109/TKDE.2013.105.
27. 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.
28. R. Chen, J. Guo, and F. Bao, “Trust Management for SOA-Based IoT and Its Application to Service Composition,” *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp. 482–495, 2016, doi: 10.1109/TSC.2014.2365797.
29. R. Chen and J. Guo, “Dynamic hierarchical trust management of mobile groups and its application to misbehaving node detection,” *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, pp. 49–56, 2014, doi: 10.1109/AINA.2014.13.
30. Y. ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent, “Trust management system design for the Internet of Things: A context-aware and multi-service approach,” *Computers and Security*, vol. 39, no. PART B, pp. 351–365, 2013, doi: 10.1016/j.cose.2013.09.001.
31. Jøsang, R. Ismail, and C. Boyd, “A survey of trust and reputation systems for online service provision,” *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007, doi: 10.1016/j.dss.2005.05.019.
32. R. Chen, F. Bao, M. Chang, and J. H. Cho, “Trust management for encounter-based routing in delay tolerant networks,” *GLOBECOM - IEEE Global Telecommunications Conference*, 2010, doi: 10.1109/GLOCOM.2010.5683235.
33. R. Chen, F. Bao, M. Chang, and J. H. Cho, “Dynamic trust management for delay tolerant networks and its application to secure routing,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1200–1210, 2014, doi: 10.1109/TPDS.2013.116.
34. U. Jayasinghe, N. B. Truong, G. M. Lee, and T. Um, “RpR: A Trust Computation Model for Social Internet of Things,” in 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016, pp. 930–937. doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0146.
35. V. Mohammadi, A. M. Rahmani, A. M. Darwesh, and A. Sahafi, “Trust-based recommendation systems in Internet of Things: a systematic literature review,” *Human-centric Computing and Information Sciences*, vol. 9, no. 1, 2019, doi: 10.1186/s13673-019-0183-8.
36. Z. C. G. Y. Y. G. Q. P. Y Wang, *A Trust Measurement in Social Networks Based on Game Theory*, vol. 9197. Cham: Springer International Publishing, 2015. doi: 10.1007/978-3-319-21786-4.
37. S. Smaldone, L. Han, P. Shankar, and L. Iftode, “RoadSpeak,” pp. 43–48, 2008, doi: 10.1145/1435497.1435505.
38. X. Hu et al., “Social drive: A crowdsourcing-based vehicular social networking system for green transportation,” in DIVANet 2013 - Proceedings of the 3rd ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, Co-located with ACM MSWiM 2013, 2013, pp. 85–92. doi: 10.1145/2512921.2512924.
39. D. Guinard, M. Fischer, and V. Trifa, “Sharing using social networks in a composable Web of Things,” in *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops 2010*, 2010, pp. 702–707. doi: 10.1109/PERCOMW.2010.5470524.
40. L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H. W. Gellersen, “Smart-its friends: A technique for users to easily establish connections between smart artefacts,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2001, vol. 2201, pp. 116–122. doi: 10.1007/3-540-45427-6_10.
41. L. Atzori, A. Iera, G. Morabito, and M. Nitti, “The social internet of things (SIoT) - When social networks meet the internet of things: Concept, architecture and network characterization,” *Computer Networks*, vol. 56, no. 16, pp. 3594–3608, 2012, doi: 10.1016/j.comnet.2012.07.010.
42. L. Atzori, A. Iera, G. Morabito, and M. Nitti, “The social internet of things (SIoT) - When social networks meet the internet of things: Concept, architecture and network characterization,” *Computer Networks*, vol. 56, no. 16, pp. 3594–3608, 2012, doi: 10.1016/j.comnet.2012.07.010.

43. Singh and A. K. Verma, "A fuzzy-based trust model for flying ad hoc networks (FANETs)," *International Journal of Communication Systems*, vol. 31, no. 6, p. e3517, Apr. 2018, doi: 10.1002/dac.3517.
44. Jiang, G. Han, C. Zhu, S. Chan, and J. J. P. C. Rodrigues, "A Trust Cloud Model for Underwater Wireless Sensor Networks," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 110–116, 2017, doi: 10.1109/MCOM.2017.1600502CM.
45. F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Trust on the ratee: A trust management system for social internet of vehicles," *Wireless Communications and Mobile Computing*, vol. 2017, 2017, doi: 10.1155/2017/7089259.
46. 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.
47. "Theory and Problems in Financial Management : M. Y. Khan : 9780074636831." https://www.bookdepository.com/Theory-Problems-Financial-Management-M-Y-Khan/9780074636831 (accessed Jul. 25, 2022).
48. M. Vegni, V. Loscri, G. Ruggeri, A. Benslimane, and K. C. Chen, "Guest Editorial Special Issue on Recent Advances on Social Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2420–2422, 2018, doi: 10.1109/JIOT.2018.2860341.
49. T. Tsao, "Fuzzy net present values for capital investments in an uncertain environment," *Computers and Operations Research*, vol. 39, no. 8, pp. 1885–1892, Aug. 2012, doi: 10.1016/j.cor.2011.07.015.
50. R. Trestian, O. Ormond, and G. M. Muntean, "Game theory-based network selection: Solutions and challenges," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4, pp. 1212–1231, 2012, doi: 10.1109/SURV.2012.010912.00081.
51. Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, "Game theory in wireless and communication networks: Theory, models, and applications," *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*, vol. 9780521196, pp. 1–535, 2011, doi: 10.1017/CBO9780511895043.
52. J. Jones, "Cooperative games," *Game Theory*, pp. 161–209, 2000, doi: 10.1533/9780857099693.161.
53. N. Nisan, T. Roughgarden, É. Tardos, and V. v. Vazirani, "Algorithmic game theory," *Algorithmic Game Theory*, vol. 9780521872, pp. 1–754, 2007, doi: 10.1017/CBO9780511800481.
54. Y. Shoham, "Computer science and game theory," *Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS*, vol. 1, pp. 1–10, 2008, doi: 10.1057/9780230280847_5.
I. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J. P. Hubaux, *Game theory meets network security and privacy*, vol. 45, no. 3. 2013. doi: 10.1145/2480741.2480742.
55. Asgharpour. MJ, Group decision making and game theory with the attitude of Operations Research., First Edition. 2003.
56. Q. Z. A. P. S. J. GAO, "COALITIONAL GAME WITH FUZZY PAYOFFS AND CREDIBILISTIC SHAPLEY VALUE," *Iranian Journal of Fuzzy Systems Vol. 8, No. 4, (2011) pp. 107-117*.
57. F. Meng and Q. Zhang, "The Shapley Value on a Kind of Cooperative Fuzzy Games," 2011. Accessed: Jul. 25, 2022. [Online]. Available: http://www.Jofcis.com1553-9105/
58. F. Meng, Y. W.-I. S. and Applications, and undefined 2012, "The Shapley value for fuzzy games on vague sets," *wseas.us*, Accessed: Jul. 25, 2022. [Online]. Available: http://www.wseas.us/journal/pdf/information/2012/54-576.pdf
59. L. Kuo, C. H. Shih, and Y. C. Chen, "Performance analysis of real-time streaming under TCP and UDP in VANET via OMNET," in *2013 13th International Conference on ITS Telecommunications, ITST 2013*, 2013, pp. 116–121. doi: 10.1109/ITST.2013.6685531.
60. F. J. Martinez, C. K. Toh, J.-C. Cano, C. T. Calafate, and P. Manzoni, "A survey and comparative study of simulators for vehicular ad hoc networks (VANETs)," *Wireless Communications and Mobile Computing*, vol. 11, no. 7, pp. 813–828, Jul. 2011, doi: 10.1002/wcm.859.
61. B. Liu, B. Khorashadi, H. Du, D. Ghosal, C. N. Chuah, and M. Zhang, "VGSim: An integrated networking and microscopic vehicular mobility simulation platform," *IEEE Communications Magazine*, vol. 47, no. 5, pp. 134–141, 2009, doi: 10.1109/MCOM.2009.4939289.
62. W. J. Liu, Y. S. Chang, C. H. Wang, G. H. Kou, and C. F. Lo, "Microarray and RT-PCR screening for white spot syndrome virus immediate-early genes in cycloheximide-treated shrimp," *Virology*, vol. 334, no. 2, pp. 327–341, Apr. 2005, doi: 10.1016/j.virol.2005.01.047.