

Dynamic Game Modeling and DNAS² Framework for Dual-S Security in Internet of Vehicles

SUN Songer¹, YU Nenghai² and LIANG Liwen^{1*}

1 H3C Technologies Co., Limited, Beijing, Beijing 100094, China

2 University of Science and Technology of China, Hefei, Anhui 230026, China

Abstract Security is of paramount importance to the Internet of Vehicles (IoV), leading to the proposal of the Dual-S architecture integrating functional safety and cybersecurity. However, complex resource competition, collaborative interactions, irreconcilable external adversarial interactions, and mutual outcome transmission across these two security levels lack a unified descriptive and analytical framework. To address this gap, we propose DNAS²—a Dual-Nature Alliance Security and Strategy Framework for IoV security—based on mainstream game theory, which consists of two interconnected core modules: in the Internal Cooperative Game Module, we formalize the Dual-S Alliance with collective rationality prioritized over individual interests, propose an equilibrium solution method for coalition benefit allocation, and prove that this method can drive the endogenous security system toward Pareto optimality; in the External Non-Cooperative Attack-Defense Game Module, we construct a model incorporating dynamic strategy evolution and information asymmetry in attack-defense confrontations, derive equilibrium solutions, and provide a mathematical basis for optimal defense strategy formulation and payoff prediction. The unified analytical tool we propose supports the optimization of IoV security schemes, and future work will focus on model refinement, exploring its applications in evolutionary game scenarios, and promoting its engineering implementation.

Keywords IoV security, Dual-S, Game Theory, Pareto Optimality, DNAS² model.

Citation SUN Songer, YU Nenghai and LIANG Liwen. Dynamic Game Modeling and DNAS² Framework for Dual-S Security in Internet of Vehicles. *Security and Safety* 2026; x: xxxxxxx.

<https://doi.org/10.1051/sands/xxxxxx>

1 Introduction

The growing popularity of intelligent connected vehicles and accelerated vehicle-road-cloud integration have propelled Internet of Vehicles (IoV) technology onto a fast development trajectory [1-2]. IoV enables intelligent traffic planning and management for significantly improved accident prevention, travel efficiency, and travel convenience. However, it also introduces new technical risks and exposure surfaces, facing challenges such as privacy breaches, driving safety threats, remote vehicle control attacks, component vulnerability exploitation, and near-field communication hijacking [3-5].

Correspondingly, the development of IoV security systems has undergone several historical stages. Before the widespread adoption of intelligent connected vehicle technology, IoV security primarily focused on vehicle safety, emphasizing functional safety (abbreviated as Safety) through in-vehicle security architectures. These security architectures were centered on physical protection, employing mechanical design, hardware safeguards, and active/passive safety technologies to prevent random hardware failures and systemic failures in electronic systems during operation, ensuring "no unreasonable risk arising from abnormal electronic system behavior [6]". The core approach at this stage was to prioritize hardware reliability design for accident prevention, and consequence mitigation, with technical logic revolving

* Corresponding author (email: liangliwen@h3c.com)

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0>),

which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.
© The Author(s), published by EDP Sciences and China Science Publishing & Media Ltd., 2026

around vehicle stability and reliability.

With the rise of intelligent connected vehicles and vehicle-road-cloud integration, alongside increasing reports of cyber intrusions, cybersecurity (abbreviated as Security) gained prominence [7-9]. It employs information/cybersecurity technologies, management, and policies to protect data, communication, computation, and control processes in IoV systems from malicious attacks, ensuring confidentiality, integrity, and availability. This mitigates threats such as control failures, privacy leaks, or traffic system paralysis due to security vulnerabilities.

As IoV security evolved into a systematic framework, the parallel integration of Safety and Security shifted the paradigm from "failure prevention" to "intrusion prevention," leading to widespread adoption of the Dual-S approach [10-12]. However, the competitive relationship and resource allocation basis between Safety and Security, as well as the confrontation between the Dual-S system and external risks, have not yet been formally modeled.

In recent years, the application of game theory has deepened across multiple fields, and several studies in the IoV domain have also adopted game theory to analyze communication schemes and resource allocation [13-16]. The emerging game theory-related models can be mainly classified into four categories: first, non-cooperative attack-defense game models, which utilize tools such as Nash equilibrium and Stackelberg game to analyze the confrontation among on-board security terminals, roadside units, and external attackers; second, cooperative game models, which rely on methods like the Shapley value to address security resource allocation and node collaboration issues, such as those in Vehicle-to-Everything (V2X) services and applications; third, hybrid game models, which explore driving efficiency in vehicle-road coordination through various game relationships, typically in vehicle platooning scenarios; fourth, evolutionary game models, which employ evolutionary stable strategies to analyze the dynamic propagation laws of security behaviors of each node in the IoV environment. These studies provide important support for the quantitative analysis of IoV security, but they generally suffer from limitations of single-scenario focus and modular separation, making it difficult to achieve dynamic correlation between endogenous collaboration and external confrontation strategies. Based on the inherent sharing, compromise, and collaboration between the Dual-S attributes, as well as the inevitable long-term irreconcilable confrontation between the IoV security defense system and external attacks, and under the premise of fully considering the mutual transmission of results between these two layers of games, this paper proposes a Dual-Nature Alliance Security and Strategy Framework (DNAS²) based on the idea of hybrid games. This framework aims to solve the problems of scattered modeling methods and lack of collaborative decision-making logic in existing IoV security research. The core contribution of this paper lies in constructing a unified modeling and decision-making framework to integrate the characteristics of two typical scenarios: the competitive-cooperative relationship between functional safety and cybersecurity within the Dual-S system, and the non-cooperative adversarial relationship between the IoV security system constructed by the Dual-S and external attackers. Furthermore, the result of the first-layer Dual-S cooperative game serves as the input for the second-layer non-cooperative game between the IoV security system and external attackers, and the result of the second-layer game between attackers and defenders, in turn, affects the resource allocation between the Dual-S in the first layer. This model fills the gap in existing IoV security research regarding the lack of global systematic analysis tools. It should be noted that the focus of this study is on the construction and application verification of the framework; no new equilibrium concept is proposed, and the derivation and analysis are conducted based on classical game equilibrium theories.

2 The DNAS² Game Model for IoV

2.1 Overview of Game Theory

Game theory is a mathematical framework for analyzing competitive or conflict-driven phenomena, also known as the theory of games. It is widely applied in military, economic, political, and social domains to model conflicts, competition, and collaboration. Key elements of the theory include players, strategies, and utility functions, with Nash equilibrium [17] as a central concept. In equilibrium, no players benefit from unilaterally changing their strategy. Games are classified as cooperative or non-cooperative by external enforcement [18], as complete or incomplete by information availability, as perfect or imperfect by historical knowledge, as static or dynamic by timing, as zero-sum or non-zero-sum by payoff structure, and

as one-shot or repeated by repetition. In cooperative games, players share a global reward function, with solutions maximizing joint strategies. In non-cooperative zero-sum games, players' payoffs are inversely related, leading to equilibria where individual payoffs are maximized. Specific solution concepts and goals depend on contextual modeling.

2.2 The DNAS² Model

DNAS² is Dual-Nature Alliance Security and Strategy Framework for IoV security. As illustrated in Figure 1, its core objective is to resolve the collaborative optimization challenge between functional security and information security (Dual-S) in IoV via a two-layer game mechanism of internal coordination and external defense.

The framework comprises two game models. The first characterizes the competitive-cooperative relationships between Dual-S components in the IoV security system, focusing on solutions balancing cooperative stability and fairness. Guided by the principle of collective rationality prioritizing individual interests, the Dual-S Alliance achieves optimal resource allocation via the payoff allocation mechanism of cooperative game theory, propelling the system toward Pareto optimality and resolving the issue of inefficient internal collaboration.

The second layer corresponds to the external non-cooperative game module, describing dynamic confrontation between the IoV security system and external attackers. In this layer, the Dual-S Alliance serves as the defender in the non-cooperative game. By incorporating factors such as action sequence, information symmetry, and scenario-specific attributes, the equilibrium solution of the game is derived using classical non-cooperative game theory. This equilibrium provides a mathematical basis for the coalition to develop optimal defense strategies, predict adversarial trends and costs, calculate attack-defense payoffs, and resolve delayed responses to external attacks.

Notably, "DNA" evokes the double-helix structure of deoxyribonucleic acid, metaphorically indicating the evolution of game types toward evolutionary games. This reflects that IoV attack-defense games will adapt to future security scenarios with DNA-like evolutionary adaptability, attaining robustness and a new equilibrium amid technological evolution and dynamic confrontation.

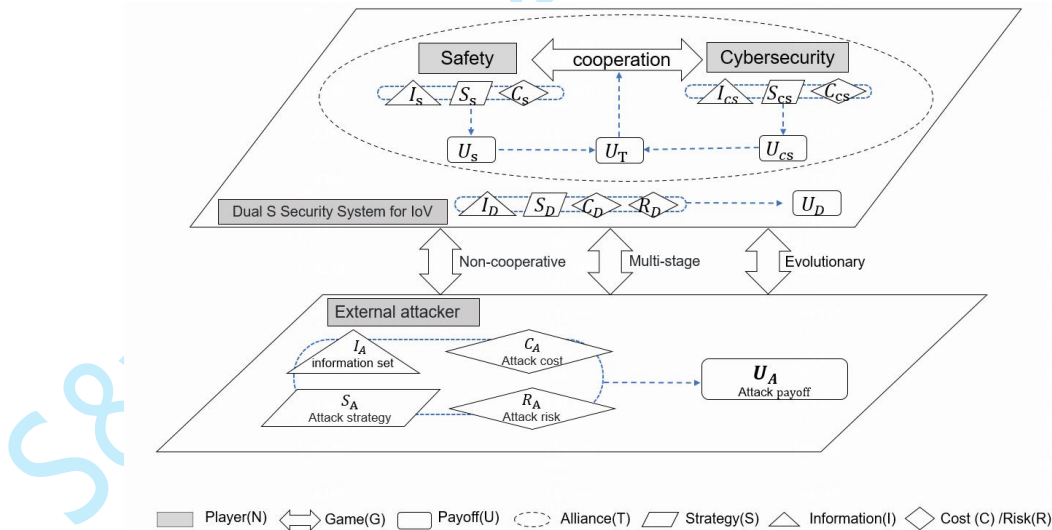


Figure 1. DNAS² Multi-Layer Game Model Framework

To implement the aforementioned game models, quantitative data support is essential for utility evaluation and resource allocation. In this study, specific quantification methods, including those for utility, rely on the normalized assignment and weighted calculation of parameters in both in-vehicle and external domains (see Figure 2). Detailed evaluation and calculation methods can refer to existing industry models, with only a schematic illustration provided in Table 1. This study focuses on utilizing such quantitative data and establishing game models for equilibrium solving to guide resource allocation, thereby providing

a rational reference for Dual-S configuration in IoV.

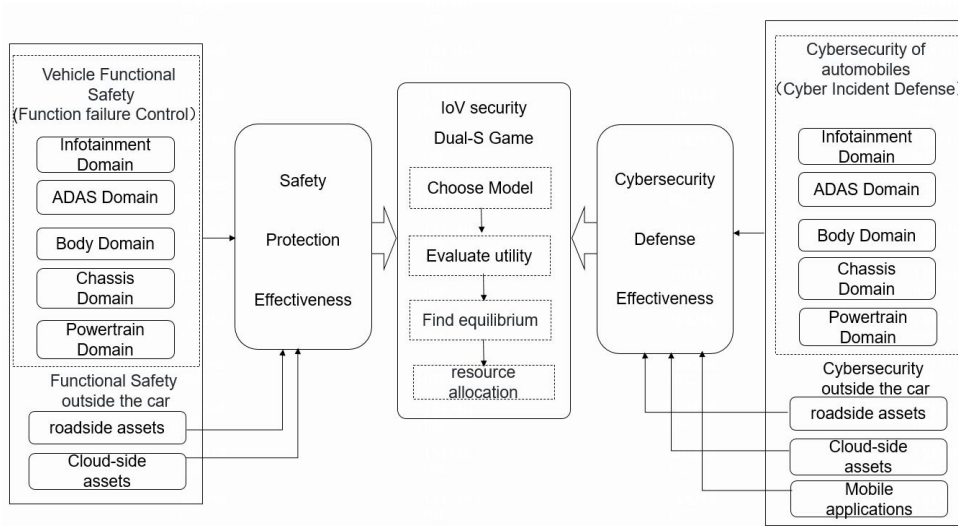


Figure 2. Components inside and outside the vehicle involved in the Dual-S cooperative game

Table 1. Mapping Table of Quantitative Indicator for Key Symbols

Key Symbol	Players	Symbol Definition	Illustrative Measurable Indicators
$u/U(\text{Payoff})$	Safety Domain, Security Domain, or Dual-S Alliance	Security benefit improvement from single-domain/co llaborative protection	<ol style="list-style-type: none"> 1. Risk Reduction Rate (Attack success probability decrease) 2. Availability Improvement Rate (Fault-free operation time proportion) 3. ASIL Compliance Rate (ISO 26262 functional safety grade compliance) 4. Relevant indicators (Industrial & enterprise requirements)
	Attacker	Direct/indirect post-attack success benefits	<ol style="list-style-type: none"> 1. Direct economic benefits (Data theft resale revenue, ransom, mining computing power gains) 2. Indirect benefits (Target node control value, core IoV data intelligence value, etc.) 3. Reputational benefits (Cybercriminal organization reputation & cooperation opportunity value conversion)
$C(\text{Cost})$	Safety Domain, Security Domain, or Dual-S Alliance	Deployment and operation & maintenance costs of components in safety/security domains	<ol style="list-style-type: none"> 1. Security device component deployment costs (e.g., hardware and software investment in IDPS/firewalls) 2. Operation & maintenance labor costs (working hours for security strategy update/vulnerability patching) 3. Fault repair costs (MTTR/MTTD×operation & maintenance unit price) 4. Relevant indicators such as other industrial and enterprise requirements
	Attacker	Total cost of resources, time, technology and other inputs for	<ol style="list-style-type: none"> 1. Attack implementation costs (Vulnerability discovery hours, attack tool procurement & development costs, attack computing power/bandwidth consumption)

		attackers' attack implementation	<ol style="list-style-type: none"> 2. Learning & preparation costs (Target system familiarization time, technical material acquisition costs) 3. Concealment costs (Proxy server fees, encrypted communication costs)
R (Risk)	Safety Domain, Security Domain, or Dual-S Alliance	Potential losses in the unprotected state	<ol style="list-style-type: none"> 1. Quantified attack loss (Economic loss assessment converted from data leakage and service interruption) 2. Risk Priority Number (RPN, calculable based on severity, occurrence and detectability) 3. Quantifiable losses such as regulatory fines and industrial disciplinary sanctions 4. Other relevant indicators such as industrial and enterprise requirements
	Attacker	Penalties, resource/benefit losses for attackers in case of attack failure or traceability	<ol style="list-style-type: none"> 1. Legal penalty costs (Fines and quantified losses from imprisonment and work suspension) 2. Resource loss costs (Value of blocked attack nodes/accounts, confiscated equipment/ransoms) 3. Opportunity loss costs (Missed potential benefits of other targets, additional costs from higher subsequent attack difficulty due to technical exposure)
Δ (Dynamic Adjustment Factor)	Dual-S Alliance	Defense Strategy Timeliness Attenuation/State Transition/Environmental Factors	<ol style="list-style-type: none"> 1. IDPS Protection Benefit Attenuation Rate (Defense rule detection rate reduction over time) 2. V2X Message Spoofing Propagation Rate (Affected proportion of surrounding nodes after single vehicle compromise) 3. Converted values of other environmental factors (bandwidth, latency, etc.)
	Attacker	Degradation of Attack Strategy Effectiveness Over Time	<ol style="list-style-type: none"> 1. 0day Exploit Benefit Attenuation Rate 2. Attack Strategy Effective Duration (Time from initial use of a specific tactic to full defense) 3. Attack Success Rate Attenuation Rate (Reduction in attack success probability per unit time due to industrial intelligence sharing) 4. Strategy Iteration Cost Growth Rate (Additional cost growth rate for attackers' strategy adjustment after defender's signature library/defense strategy update)

3 Analysis of Dual-S Cooperative Game Characteristics and Equilibrium Solutions

3.1 Analysis of IoV Cooperative Game Characteristics in Dual-S

The core of cooperative games lies in players achieving maximized collective interests through coalitions under external coercive forces. In a cooperative game, players can form coalitions, negotiate strategies, and distribute shared payoffs to achieve better outcomes than acting alone. The Dual-S meets the characteristics of cooperative games primarily in the following six aspects:

1. Partial Goal Alignment

The functional safety and cybersecurity, as game players, have certain goal conflicts. For instance, Safety ensures the reliability of vehicles and parts to minimize system failure rates and enables degradation to a safe state during failures, while Security ensures the integrity of vehicles, parts, and roadside-cloud infrastructure against hacker attacks. However, they both share the core goal of ensuring "zero accidents"

in driving safety, leaving room for Pareto improvement through cooperation.

2. Synergistic Interests

Functional safety addresses random hardware failures, while cybersecurity tackles malicious human attacks. Cooperation enables comprehensive risk matrix coverage and generates added value such as early warnings and post-incident traceability, with total payoffs exceeding the sum of individual actions, i.e., satisfying Superadditivity. For instance, when cybersecurity probes detect illegal intrusion into the powertrain domain, they can notify the functional safety system to adjust control strategies, degrade functions, slow down, or brake to avoid collision risks. After a vehicle is compromised by external intrusion, the Security system can analyze comprehensive data in the network probe context to identify the intrusion origin, reconstruct attack paths, and even identify attackers through log correlation and intelligence expansion.

3. Transferable and Allocable Payoffs

Within the alliance formed by Dual-S, payoffs—mainly including computing power, bandwidth, storage resources and update windows—can be freely allocated among participants. Resource idleness during stable operation can be regarded as the payoffs guaranteed by the Dual-S system. Idle resources during stable operation can be regarded as gains ensured by the Dual-S system. In low-risk scenarios like parking or charging, more resources can be allocated to cybersecurity for malicious file scanning, while in high-risk scenarios like high-speed driving or autonomous driving, functional safety is prioritized to meet quick real-time driving responses. Thus, resource allocation is dynamically adjusted to distribute security payoffs between players.

4. Negotiation and Bargaining Mechanisms

Safety and Security each rely on low latency, high reliability, and strong encryption-based verification, leading to conflicts and negotiations over resources such as bandwidth, latency, and computing power. Given the security level of the scenario, the two players can negotiate, for example, through the Nash bargaining solution or Shapley value allocation, to reach an agreement on the final strategy during cooperation.

5. Long-Term Interaction and Repeated Games

The rapid development of automotive electronics, electrical systems, and network technologies, along with ongoing security challenges, ensures that the Dual-S protection system will persist. Players must consider long-term cooperative gains rather than one-time games. As in-vehicle code grows exponentially and exposure surfaces expand due to vehicle-road-cloud interactions, the Dual-S will adapt to new technologies and challenges while creating new resource requirements and interaction constraints, necessitating negotiated adjustments in long-term cooperation for system-wide optimal solutions.

6. External Enforcement Forces

Literature [19] ISO 21434 explicitly requires coordinated consideration of cybersecurity and functional safety. Literature [20,21] UN R155 and R156 provide guidance and supervision for automotive cybersecurity and mandatory safety design. Literature [22,23] includes China's mandatory standards GB 44495 "Technical Requirements for Vehicle Information Security" and GB 44496 "General Technical Requirements for Vehicle Software Updates." Laws, regulations, and standards serve as external rules to enforce sustained cooperation between the Dual-S.

3.2 Formal Definition of IoV Cooperative Game

To construct the Dual-S cooperative game model for IoV and guide resource allocation, this work makes prerequisite assumptions about the rationality and overall goal gains of the Dual-S as game players, further clarifying game rules, strategy interactions of players, and their gain relationships.

Assumption 1: The functional safety and information security deployments in IoV are independent and rational, pursuing optimal strategies for players.

Assumption 2: Functional safety and information security can achieve common goals and distribute shared payoffs through cooperation.

Assumption 3: Functional safety and information security are both essential game participants. The rationality of this assumption is jointly guaranteed by IoV security compliance requirements (ISO 26262, ISO/SAE 21434) and the paper's core research objectives. Thus, scenarios with an empty alliance set or degradation into a single participant are not involved in this paper's discussions.

Definition: The IoV Safety and Security Cooperative Coalition Game (IoV-S²CG) model is defined as IoV-S²CG= (N, T, S, u, v) . Element N represents the game player set, Element T represents the Dual-S Alliance, Element S represents the strategy space of both sides, Element u and v denote the bilateral individual payoff function and the coalition payoff characteristic function, respectively.

(1) Player set N

The model contains two players: functional safety and information security. For clarity, use s to denote IoV functional safety as player 1, and use cs to denote cybersecurity as player 2. $N = \{s, cs\}$.

(2) Alliance T

Modeling Safety and Security as an alliance is key to embodying "cooperative games." Based on Assumption 3, we define $T = \{s, cs\}$ and $v(T)$ is hereinafter used to denote the overall defense payoff of the IoV security system after the coalition is formed.

(3) Strategy Space S

S represents the strategy space of both players, encompassing all possible action plans of alliance members Safety and Security. For player 1, it is defined as $S_s = \{s_1, s_2 \dots s_n\}$, where each element represents an action such as fault tolerance, function degradation, or emergency braking. For player 2, it is defined as $S_{cs} = \{cs_1, cs_2 \dots cs_n\}$, where each element represents an action such as system vulnerability scanning, patching, or file scanning and killing.

(4) Player Payoff Function u

$u(\{s\})$ denotes the payoff of independent deployment of functional safety, while $u(\{cs\})$ denotes the payoff of independent deployment of cybersecurity. Such payoffs can be statistically quantified in specific scenarios by referring to relevant standards, with considerations of metrics including event rate, mitigation time, system availability duration, attack robustness, and recovery time.

(5) Coalition Payoff Characteristic Function v

As required in game theory, the overall payoff is uniquely characterized by the coalition payoff function v . $v(T) = v(\{s, cs\})$ represents the total payoff from cooperation.

3.3 Decision-Making Methods for the IoV Cooperative Game Model

The core of decision-making in the Dual-S cooperative game for IoV lies in how the Dual-S achieve stable cooperation through alliance formation and payoff distribution. Common decision-making methods include finding the core solution (Core) and the Shapley value, which guide the allocation of resources for Safety and Security based on marginal contributions in different scenarios.

The process is as follows: first, identify the existence of cooperation conditions; second, compute the cooperative value and players' marginal contributions; finally, further derive the Shapley value to find the unique fair allocation based on marginal contributions, and simultaneously compute the "Core" to find stable allocation solution sets. If the Shapley value lies within the Core, it is the unique solution balancing cooperative stability and fairness. The following are the formulas used in this process:

Verify Superadditivity, i.e., the existence of conditions for cooperation (existence of a cooperation "Core"), with the following formula:

$$v(T) \geq \sum_{i \in N} u(\{i\}) \quad (1)$$

The alliance's synergetic gain ΔR is calculable via Equation (2) to quantify cooperative value, where Δ stands for increment and R for the alliance's security payoff. This variable represents the total payoff increment of the Dual-S subsystems in a cooperative alliance versus the sum of their independent payoffs, reflecting the IoV security performance improvement by alliance synergy. A positive ΔR is the core premise for Dual-S Alliance formation and a key input to cooperative game payoff allocation mechanisms (e.g., the Shapley value). Calculate the players' marginal contributions using formula (3).

$$\Delta R = v(T) - \sum_{i \in N} u(\{i\}) \quad (2)$$

$$MC_i(T) = v(T \cup \{i\}) - v(T) \quad (3)$$

Here, $v(T)$ is the payoff function for alliance T , and $v(T \cup \{i\})$ represents the alliance payoffs after player i joins the alliance.

Calculate the Shapley value to derive the fair allocation scheme. The Shapley value is the weighted average of player i 's marginal contribution to the alliance, calculated as:

$$\varphi_i(v) = \sum_{T \in \{s, cs\}\{i\}} \frac{|T|!(n-|T|-1)!/n!}{n!} [v(T \cup \{i\}) - v(T)] \quad (4)$$

Under the premise of Core existence, use formula (5) to compute the Core solution set:

$$\text{Core} = \{(x_s, x_{cs}) \mid x_i \geq u(\{i\}), n \cdot x = v(T)\} \quad (5)$$

Where, x_i represents the payoff allocated to a player, x represents the average of all players' payoffs, and n represents the number of players.

In summary, the decision-making algorithm flow for the cooperative game is as follows (see Figure 3).

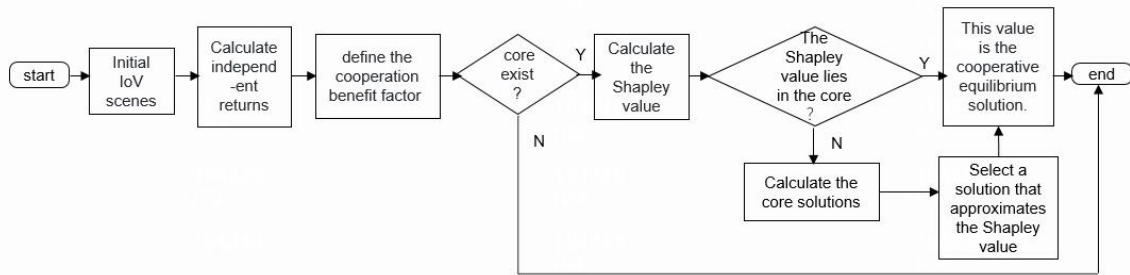


Figure 3. Decision-making process for solving the cooperative game

3.4 Derivation and Implications of Scenario-based Strategies

To intuitively verify the superadditivity of the alliance and the calculation method for members' contributions, an illustrative numerical example is constructed as follows: Assume that in the infotainment domain system of a certain vehicle model, the standardized protective payoff of deploying the functional safety component independently is 3, and that of deploying the information security component independently is 4; when the Dual-S components are deployed simultaneously and operate collaboratively, the standardized total protective payoff is 10. This example is only intended to clearly demonstrate the verification process and does not represent the measured data of any specific vehicle model.

Given $u(\{s\}) = 3$, $u(\{cs\}) = 4$, and $v(T) = 10$, verify the Superadditivity of cooperation using formula (1): $v(\{s, cs\}) = 10$, $u(\{s\}) + u(\{cs\}) = 7$, $10 > 7$. Then, calculate the synergy payoffs and marginal contributions. According to formulas (2) and (3), $\Delta R = v(T) - \sum_{i \in N} u(\{i\}) = 10 - (3 + 4) = 3$, and the marginal contribution of player s to the alliance is $10 - 4 = 6$, while the marginal contribution of player cs to the alliance is $10 - 3 = 7$. Substitute into formula (4) to calculate the Shapley value, as follows:

$$\varphi_s = \frac{3 + (10 - 4)}{2} = 4.5, \quad \varphi_{cs} = \frac{4 + (10 - 3)}{2} = 5.5$$

If Superadditivity is successfully verified, the necessary condition for a non-empty Core is satisfied. Substitute into formula (5) to calculate the Core range as all allocations satisfying $x_s \geq 3$, $x_{cs} \geq 4$, and $x_s + x_{cs} = 10$, such as (4,6) and (4.5,5.5). That is, the "Core" is the line segment $\{(x, 10x) \mid 3 \leq x \leq 6\}$. Because the Shapley value (4.5,5.5) lies within the Core, this Shapley value is the solution that satisfies both fairness and stability.

The practical significance of establishing a cooperative game model is that, although the Dual-S inevitably share and compete for limited resources, the cooperative game can be used to quantify their value and guide resource allocation based on players' contributions to the "Dual-S Alliance", as long as the cooperation of functional safety and cybersecurity can yield higher overall payoffs. If the Shapley value lies within the Core, the cooperation also has the fairest allocation that balances stability. The cooperative game promotes alliance stability and maximizes payoffs by quantifying marginal contributions of both players and establishing the relationship between allocable resources and each player's contribution, providing a mathematical basis for alliance stability. From the above process, we can infer that there are at least two ways for functional safety or cybersecurity as players to obtain more allocable resources: one

player optimizes technical solutions to improve its contribution to the alliance, thereby increasing its subsequent proportion of allocated resources, or both players emphasize and strengthen collaborative coordination. Even if their individual contributions remain unchanged, better overall collaboration (greater total alliance payoffs) will also lead to increased resources for both players, including allocated bandwidth, computing power, and investments.

4 Analysis of DNA Non-Cooperative Game Characteristics and Equilibrium Solutions

4.1 Analysis of Non-Cooperative Game Characteristics in IoV Attack and Defense

The IoV security defense system built based on the Dual-S model faces long-term challenges from external attackers. In confrontation, the attack and defense sides exhibit clear non-cooperative game characteristics [23, 24], mainly manifested as opposing goals, interdependent strategies, explicit payoff functions, information asymmetry, and the existence of equilibrium solutions in most cases.

1. Conflicting goals

In the security confrontation of IoV, both attackers and defenders have clear objectives. For instance, intruders aim to seize vehicle control rights by constructing various attack vectors, while the IoV security defense system controls, detects, and mitigates potential security risks through various technical means. The goals of both sides are completely opposed, and the conflict of their interests is irreconcilable.

2. Mutual influence of strategies

Non-cooperative games require each player to have a clear set of strategies, which are selectable action plans. In the IoV security system, the defender's strategies include using dynamic authentication mechanisms, traffic encryption, redundant physical part design, and access control, while the attacker's strategies include CAN bus cracking, channel eavesdropping, planting vehicle malware, or exploiting part vulnerabilities. Both sides must fully consider the opponent's strategies, conduct rational global analysis, and practice empathy when selecting their own strategies, as the final outcome is jointly determined by both parties' strategies.

3. Clear utility function

Both sides in the IoV attack-defense game seek to maximize payoffs and minimize costs and risks in their actions. The final utility function is the net payoff after "benefit - cost (+ risk)."

4. Asymmetric information structure

Based on players' knowledge of game information, non-cooperative games are classified into two categories: games of complete information and games of incomplete information. "Complete information" games require both sides to know each other's strategy space and payoff function, a game where one party conceals partial information is called an "incomplete information game," such as the use of private encryption algorithms in vehicle-to-everything communication, attackers exploiting undisclosed 0-day vulnerabilities, and potential new techniques and tactics of APT(Advanced Persistent Threat).

5. Existence of equilibrium solutions

Almost all IoV attack-defense scenarios with finite strategies have at least one Nash equilibrium (including pure or mixed strategy equilibria). Most IoV attack-defense scenarios fall under "incomplete information games," which can be transformed into "complete information games" for analysis by introducing a "belief system" via Harsanyi transformation. Thus, most IoV attack-defense scenarios have Nash equilibria and their variants (e.g., subgame perfect equilibrium, Bayesian equilibrium, etc. [23-25]).

4.2 Formal Definition of IoV Non-Cooperative Games

To build a non-cooperative game model between the IoV security system and external attackers and guide decision-making, this work makes preliminary assumptions about the rationality and limited resources of both sides as game players.

Assumption 1: The IoV security defense side (Dual-S Alliance) and the external attacker side are two rational game players. Both make rational decisions, aiming to maximize their respective payoffs through strategy selection, and both engage in a dynamic process to seek their optimal strategies.

Assumption 2: Both attack and defense sides make decisions and act under limited resources, constrained by capabilities, resources, and preferences. Their strategies must balance needs and resource adaptability.

Definition: The non-cooperative game model for IoV security attack-defense, IoV-DANG (IoV-DA

Non-cooperative Game), is defined as $\text{IoV-DANG} = (N, S, \theta, P, K, \Delta, U)$. The seven-tuple consists of participants, strategy space, type space, type prior distribution, dynamic game stages, dynamic adjustment factors, and final utility.

(1) Player set N

Use D to denote the defense side (the IoV Dual-S system), and use A to denote external hackers or attackers. The player set $N = \{D, A\}$.

(2) Strategy space S

Define S_D as the set of defense strategies, which may include CAN bus encryption, security chips, onboard intrusion detection and prevention systems (IDPS), and cloud-based security protection. This set is formally expressed as $S_D = \{d_1, d_2, \dots, d_m\}$. Similarly, define S_A as the set of attack strategies, which may include side-channel attacks, fault injection, vulnerability mining, and malicious code implantation. This set is formally expressed as $S_A = \{a_1, a_2, \dots, a_n\}$.

(3) Type space θ

Different from the strategy space, the type space refers to players' intrinsic private characteristics unobservable externally. It is defined as $\theta = \theta_D \cdot \theta_A$, where $\theta_D = \{\theta_{D1}, \theta_{D2} \dots \theta_{Dn}\}$, $\theta_A = \{\theta_{A1}, \theta_{A2} \dots \theta_{Am}\}$.

The intrinsic attributes of players can be categorized by a single dimension or multiple integrated dimensions, thereby defining their type spaces. For example, if the players in a certain game are the defender represented by the cloud control platform and the attacker represented by a cyber intrusion group, the types of defenders can be simply divided into two categories: those with strong security awareness that update defense feature libraries in a timely manner and deploy new defense methods are denoted as θ_{DH} ; those with weak security awareness that mostly adopt weak passwords and outdated components are denoted as θ_{DL} . Then the defender type space is expressed as $\theta_D = \{\theta_{DH}: \text{high defense level}, \theta_{DL}: \text{low defense level}\}$. Similarly, the attacker type space can be defined based on the maturity of tactics and techniques, organizational visibility, zero-day vulnerability exploitation capabilities and platform-based engineering capabilities. Advanced attackers (e.g., APT groups) are denoted as θ_{AH} , and ordinary ones (e.g., hackers or cybercrime gangs) as θ_{AL} . In this case, the attacker type space can be expressed as $\theta_A = \{\theta_{AH}: \text{APT group}, \theta_{AL}: \text{hacker gang}\}$.

It should be noted that a type space is characterized by being privately known to insiders yet confidential to external parties, and must be used in conjunction with the prior type distribution P .

(4) Type prior distribution P

P defines the common belief of all players regarding each other's private types prior to the start of a game. $P(\theta)$ denotes the unanimously agreed-upon probability distribution of the type combinations for all players, i.e., the probability distribution of the occurrence of $\theta = \{\theta_1, \theta_2 \dots \theta_n\}$. In other words, it represents a player's initial probabilistic judgment of the other party's type based on industry data or historical experience, and must satisfy the probability normalization property, expressed as $\sum P(\theta_i) = 1$.

For the game scenario described above, if the defender infers through professional analysis that the probability of the intruder being a high-capability targeted attacker θ_{AH} is 30% and the probability of being a low-capability hacker gang θ_{AL} is 70%, then $P(\theta_{AH}) = 0.3$ and $P(\theta_{AL}) = 0.7$ constitute an a priori probability judgment. Meanwhile, through prior intelligence collection, the attacker also forms an a priori belief about the defender with $P(\theta_{DH}) = 0.4$ and $P(\theta_{DL}) = 0.6$. In this case, the joint probabilities are given by: $P(\theta_{DH}, \theta_{AH}) = 0.12$; $P(\theta_{DH}, \theta_{AL}) = 0.28$; $P(\theta_{DL}, \theta_{AH}) = 0.18$; $P(\theta_{DL}, \theta_{AL}) = 0.42$. These joint probabilities directly influence the strategy selection of both parties in the game and serve as the starting point for Bayesian inference. Therefore, P represents the probabilistic cognition of the type boundaries of game players, and the formulation of θ and P constitutes the core logic of incomplete information games.

(5) Game stage set K

$K = \{K_1, K_2 \dots K_n\}$ denotes the set of game stages that are incurred by environmental changes in dynamic IoV A&D games, such as a single static game ($K=1$), a finite repeated game ($K>1$), and an infinite-stage game ($K=\infty$).

(6) Dynamic adjustment factor Δ

Δ describes the disturbance of payoffs induced by environmental changes and the impact of state transitions in multi-stage games, including the attenuation of current payoffs by historical strategies. Examples include the protective benefits of in-vehicle IDPS deployed in earlier stages against subsequent attacks, and the V2X message spoofing potentially caused by the compromise of a single vehicle. This

factor underscores the temporal dependence of strategies and the cross-stage transmission of payoffs, and can be expressed as $\Delta(K) = e^{-\lambda K} + \delta$. K denotes the game stage, and $e^{-\lambda K}$ represents the exponential attenuation term of historical strategies where $\lambda > 0$ is the attenuation coefficient (e.g., corresponding to the attenuation of IDPS protective effectiveness or zero-day attack impact). δ refers to the comprehensive dynamic disturbance term that incorporates factors such as state transitions and environmental fluctuations—for instance, $\delta = -0.3$ in the event of a single vehicle compromise, and $\delta = 0$ under stable environmental conditions.

(7) Players' payoff function U

Calculating the payoff function requires introducing the concepts of cost, benefit, and risk. Cost C includes defense resource overheads and upgrade costs, attack weapon development, persistence costs, and vulnerability mining costs. Benefit B refers to the basic benefit brought by successful strategy execution. Risk R includes the losses suffered by the defender after being compromised, as well as the economic and legal risks the attacker must bear after a failed attack. The benefits for both sides can be expressed as:

$$U_i = B - C - R + \Delta_i U_i(t-1) \quad (6)$$

Defender's benefit:

$$U_D(S_d, S_a, t) = B_D - C_D(S_d, t) - R_D(S_d, t) + \Delta_D U_D(t-1) \quad (7)$$

Attacker's benefit:

$$U_A(S_a, S_d, t) = B_A - C_A(S_a, t) - R_A(S_a, t) + \Delta_A U_A(t-1) \quad (8)$$

4.3 Decision-Making Methods for Non-Cooperative Models in IoV

The attack-defense confrontation scenarios in IoV and their corresponding game types can be summarized as follows (see Table 2).

Table 2. Typical Classification and Solution of Non-Cooperative Games in IoV Attack-Defense Confrontation

Type	Examples	Typical Solution Methods and Tools
Complete information static game	Symmetric key cracking, frequency spectrum signal interference, public DoS attacks ...	Schelling game payoff matrix, combined with the underline method and reaction function to solve for the Nash equilibrium
Incomplete information static game (static Bayesian game)	False signal injection, one-time infection of in-vehicle infotainment worms, acquisition of SRC 0-day vulnerabilities by automakers, man-in-the-middle attacks...	Use Harsanyi transformation, introduce "nature," quantify uncertainty through prior beliefs, and then solve for the Bayesian Nash equilibrium
Complete information dynamic game	Ransomware attacks, OTA updates, V2X message verification, vulnerability remediation...	Build a game tree and use backward induction to find the subgame perfect Nash equilibrium (SPNE)
Incomplete information dynamic game (dynamic Bayesian)	CAN encryption matrix cracking, 0-day vehicle control attacks, multi-stage phishing attacks, APT attacks, antivirus evasion,	Use Bayesian dynamic belief updates, sequential optimization strategies, supplemented by reinforcement learning, game trees, etc., to solve for

game)	honeypot trapping...	the perfect Bayesian equilibrium (PBE)
-------	----------------------	--

A complete information game can be used to solve for the Nash equilibrium. If a strategy pair (S_d^*, S_a^*) in the game satisfies the following conditions, then this strategy pair is the Nash equilibrium solution for the game.

$$\left. \begin{aligned} U_D(d^*, a^*) &\geq U_D(d, a^*), \forall d \in S_D \\ U_A(d^*, a^*) &\geq U_A(d^*, a), \forall a \in S_A \end{aligned} \right\} \quad (9)$$

In most cases, there is no pure strategy Nash equilibrium in actual IoV attack-defense game scenarios. Instead, multiple rounds of confrontation are needed to solve for a mixed strategy Nash equilibrium. In a typical Stackelberg game model, players consist of a leader and a follower. The leader has the first-mover advantage and determines their mixed s

strategy first, such as which defense strategies to deploy and the probabilities of using each strategy combination. The attacker, as the follower, observes and selects the strategy that maximizes their payoffs. Let p denote the leader's (defender's) mixed-strategy probability ($p_i \in [0,1]$), and q represent the follower's (attacker's) mixed-strategy probability ($q_i \in [0,1]$), the payoff functions for both sides can be expressed as:

$$\left. \begin{aligned} U_D(p, q) &= \sum_{i \in S_D} \sum_{j \in S_A} U_D(d_i, a_j) \cdot p_i \cdot q_j \\ U_A(p, q) &= \sum_{i \in S_D} \sum_{j \in S_A} U_A(d_i, a_j) \cdot p_i \cdot q_j \end{aligned} \right\} \quad (10)$$

Another feature of IoV attack-defense scenarios is the possible existence of information asymmetry. Although automakers may know that attackers could be internal employees, external individuals, cybercrime organizations, or even state-sponsored APT groups, and may even know the probability of each attack type, they may not know the specific type of attacker in each incident. In this case, solving for a Bayesian Nash equilibrium is required. This involves using Harsanyi transformation to introduce "nature" to set the distribution probability for the strategy type θ of a player. Let the strategy types of both sides be θ_D and θ_A , where $\theta_D = \{\theta_{D1}, \theta_{D2}\}$ (simply representing strong protection or weak protection), and $\theta_A = \{\theta_{A1}, \theta_{A2}\}$ (simply representing conventional or advanced attacks). Then, P_D and P_A denote the probability spaces for strategy types of players, where, $P_{Di} = \{P_{D1}, P_{D2}\}$ with $\sum_{i=1}^2 P_{Di} = 1$, $\theta_{D1} = \{d_1, d_2, d_3\}$ corresponds to OTA upgrade, virus detection, and behavior anomaly detection, and $\theta_{D2} = \{d_4, d_5, d_6\}$ corresponds to OTA upgrade disabled, weak encryption in communication, and simple whitelist-based filtering. $P_{Ai} = \{P_{A1}, P_{A2}\}$, with $\sum_{j=1}^2 P_{Aj} = 1$, $\theta_{A1} = \{a_1, a_2, a_3\}$ corresponds to fileless attacks, 0-day attack, and anti-virus evasion), and $\theta_{A2} = \{a_4, a_5, a_6\}$ corresponds to scan probing, N-day exploit, and normal virus attacks. The payoff function can then be expressed as:

$$\left. \begin{aligned} U_D(t) &= \sum_{\theta_D} P_{Di} \cdot P_{Aj} \cdot U_D(d_i, a_j) \\ U_A(t) &= \sum_{\theta_A} P_{Di} \cdot P_{Aj} \cdot U_A(d_i, a_j) \end{aligned} \right\} \quad (11)$$

$$U_D^*(t) = \max \sum \{ P(a_j | d_i) U_D[(D(t), A^*(t)), d_i, a_j] \} \quad (12)$$

$$U_A^*(t) = \max \sum \{ P(d_i | a_j) U_A[(A(t), D^*(t)), S_a, S_d] \} \quad (13)$$

By jointly solving equations (11-13) using linear programming or game analysis tools (Gambit or Python libraries), we obtain U_D , U_A , and the corresponding Bayesian Nash equilibrium solution $EQ(S_b^*(t), S_a^*(t))$. The decision-making process for non-cooperative game solving is as follows (see Figure 4).

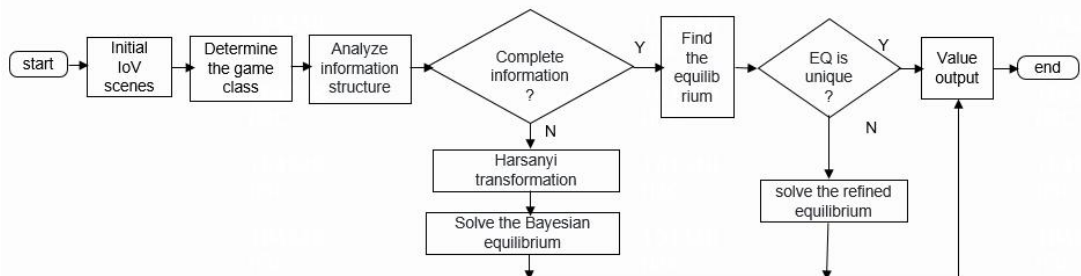


Figure 4. Non-cooperative game-solving decision process

4.4 Derivation and Implications of Scenario-based Strategies

Scenario 1: Vehicle-cloud communication confrontation scenario. Through mathematical modeling, find the mixed equilibrium under multiple channel hijackings, and observe the interaction between the attack and defense strategies and payoffs in the IoV.

Assumption 1: Players are defender D and attacker A . Both sides have a shared understanding of their strategy spaces and payoff functions and engage in continuous channel hijacking confrontation in the vehicle-cloud communication scenario.

Assumption 2: For the sake of computational simplification, it is assumed that the attacker's brute-force cracking technology achieves a 100% success rate in attacking plaintext channels, and quantum cracking technology achieves a 100% cracking rate for both encrypted and plaintext channels.

Definition 1: The defender may select plaintext transmission with probability p and encrypted transmission with probability $(1-p)$ to balance efficiency and security. Correspondingly, the attacker may choose brute-force cracking with probability q and quantum resistance with probability $(1-q)$ to balance costs.

Definition 2: The defender's cost for deploying plaintext and encrypted channels is $C_d = \{C_{d1}, C_{d2}\}$, and the attacker's cost for dictionary attacks and quantum resistance devices is $C_a = \{C_{a1}, C_{a2}\}$.

Definition 3: The attacker's payoff for successful communication cracking is $Y_a, Y_A = \{Y_a\}$, corresponding to the defender's loss (negative payoff) for information leakage as Y_d . The defender's payoff for successfully securing vehicle-cloud communication is Y_y , so the defender's payoff is $Y_D = \{-Y_d, Y_y\}$.

Thus, the final payoff function for the players can be expressed as $U_i(D, A) = Y_i - C_i (i \in \{d, a\})$. Solve for the game equilibrium: $EQ(S_D^*, S_A^*)$.

Table 3. Payoff matrix for attack-defense confrontation

	Brute force (BF)	Quantum resistance (QR)
Plaintext Transmission (PI)	$-C_{d1}-Y_d, Y_a-C_{a1}$	$-C_{d1}-Y_d, Y_a-C_{a2}$
Encrypted communication (En)	$Y_y-C_{d2}, -C_{a1}$	$-C_{d2}-Y_d, Y_a-C_{a2}$

Based on empirical observations in cybersecurity, the cost for a defender to deploy encrypted communication exceeds that of maintaining a plaintext channel. Furthermore, the cost for an attacker to employ quantum-cracking equipment is substantially higher than that of using brute-force cracking tools. Concurrently, the inherent risk of communication data breach arising from channel-decryption confrontations must be considered. Therefore, for a specific vehicle-cloud communication confrontation scenario, it can be hypothesized that the core parameters are characterized by the upfront deployment costs for both attackers and defenders, the payoffs from successful channel compromise (hijacking) and unsuccessful attacks (transmission security), and the risk of communication data breach, which can be quantified as: $C_{d1}=3, C_{d2}=5, C_{a1}=1, C_{a2}=10, Y_a=Y_d=20$, and $Y_y=10$. The payoff matrix based on these settings is shown in Table 4. The underline method reveals that a pure strategy equilibrium is not available for this game, necessitating further solving for a mixed Nash equilibrium.

Table 4. Quantified payoff matrix for attack-defense confrontation

	Brute force (BF)	Quantum resistance (QR)
Plaintext Transmission (PI)	<u>-23, 19</u>	<u>-23, 10</u>
Encrypted communication (En)	<u>5, -1</u>	<u>-25, 10</u>

Based on the defender's payoff formula (10), we derive:

$$U_D = (-C_{d1}-Y_d)pq + (-C_{d1}-Y_d)p(1-q) + (Y_y-C_{d2})(1-p)q + (-C_{d2}-Y_d)(1-p)(1-q)$$

At this point, the optimal strategies for each party can be calculated by setting the first-order derivative of

each party's payoff with respect to their decision variables (probabilities) to zero, or by listing equations based on the definition of Nash equilibrium, such as "regardless of the attacker's strategy, the payoffs corresponding to the defender's two strategies are equal," as expressed below:

$$U_{DPl}=(-C_{d1}-Y_d)q+(-C_{d1}-Y_d)(1-q)=(Y_y-C_{d2})q+(-C_{d2}-Y_d)(1-q)=U_{DEn}$$

Rearranging terms yields:

$$q=\frac{C_{d1}-C_{d2}}{Y_y+Y_d}, 1-q=\frac{Y_y+Y_d+C_{d1}-C_{d2}}{Y_y+Y_d}$$

This represents the optimal action probability for the attacker using ordinary brute force and quantum resistance. Similarly, the defender's probability p can be calculated based on the attacker's payoff function using formula (10):

$$U_{ABF}=(Y_a-C_{a1})p+(-C_{a1})(1-p)=(Y_a-C_{a2})p+(Y_a-C_{a2})(1-p)=U_{AQR}$$

Rearranging terms yields:

$$p=\frac{Y_a-C_{a2}+C_{a1}}{Y_a}, 1-p=\frac{C_{a2}-C_{a1}}{Y_a}$$

Substituting the data, we find $q=1/15$ and $p=11/20$ as the optimal action probabilities for both parties. Further calculations of their payoffs U_D and U_A show that $U_D=-C_{d1}-Y_d=-23$, $U_A=Y_a-C_{a2}=10$ are their expected payoffs.

Thus, in this encryption game scenario, the defender randomly uses plaintext and encryption at an 11:9 ratio, while the attacker randomly uses ordinary brute force and quantum resistance measures at a 1:14 ratio, forming a mixed Nash equilibrium in this vehicle-cloud communication hijacking game.

Additionally, based on $1-p=\frac{C_{a2}-C_{a1}}{Y_a}$, $q=\frac{C_{d1}-C_{d2}}{Y_y+Y_d}$

And $U_D=-C_{d1}-Y_d=Y_a-C_{d1}$, $U_A=Y_a-C_{a2}$, we derive the following inferences:

The strategy choices (probabilities) of both parties are composite functions of each other's action costs and payoffs, indicating that both must fully consider the opponent's action costs and values when formulating strategies.

The payoffs of both parties are closely tied to the importance of the protected assets. In the contest for control over specified assets, reducing the defender's basic defense costs or the attacker's high-order attack costs can increase their respective payoffs. That is, the defender's final payoff is determined by the cost of basic defense, while the attacker's final payoff is determined by the cost of deploying high-order attack tools.

Scenario 2: The Automaker is developing strategies to deploy intrusion detection and protection system (IDPS). We can use mathematical models to analyze how changes in players' strategies affect the adversarial dynamics and influence outcomes.

Assumption 1: A specific IVI system supports either A defense component or B defense component, with only one enabled at a time, switchable via OTA updates. The A defense component with a 60% detection rate for known (N-day) IVI vulnerabilities and 30% for unknown attacks (0-day exploits). The B defense component improves the 0-day exploit detection rate to 90%, but 20% identification rate for known vulnerabilities, as shown in Table 5.

Assumption 2: As the defender, the automaker's payoff is defined by the vehicle's security level, which is quantified as the intrusion detection rate. In this model, the attacker's payoff is the opposite of the defender's. Thus, the interaction constitutes a zero-sum game (ZSG), where we consider only the binary outcomes of actions (success or failure) and abstract away from implementation costs.

Below are the optimal strategies and calculations for both the attacker and defender in this scenario.

Table 5. Payoff matrix for the vulnerability game

	Known vulnerabilities (N-day)	Unknown vulnerabilities (0-day)

A defense component	60, -60	30, -30
B defense component	20, -20	90, -90

Using formula (10) and the payoff equation, we calculate p , q , U_A and U_D . Figure 5 presents the game-theoretic analysis from the defender's perspective. As shown in the figure, when the probability that the automaker deploys B defense components falls below 30%, the attacker's optimal strategy is to concentrate on using 0-day exploits to maximize their intrusion success rate; conversely, when this probability exceeds 30%, the attacker tends to reduce the reliance on 0-day exploits. The intersection of the two curves represents the "fixed point" of the game. Specifically, when the automaker adopts a mixed strategy of randomly upgrading A defense or B defense components in a 3:7 ratio, the system's threat detection rate reaches and stabilizes at 48%. Any deviation from this equilibrium strategy will trigger adaptive adjustments by the attacker, thereby altering the outcome of the game.

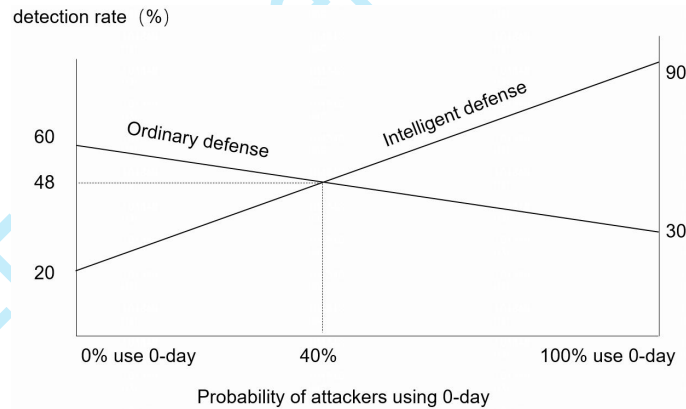
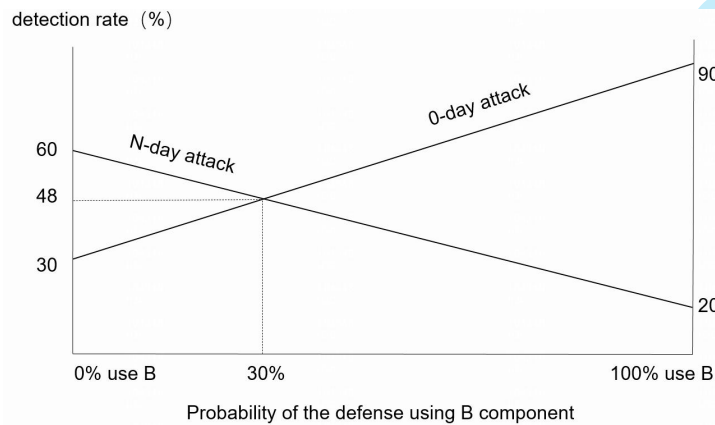


Figure 5. Mixed Strategy Outcome Analysis-1

Figure 6. Mixed Strategy Outcome Analysis-2

Figure 6 reveals the optimal strategy from the attacker's perspective: employing 0-day exploits with a 40% probability. At this equilibrium point, regardless of the type of defense components deployed in the vehicle, the average interception rate remains fixed at 48%. Any deviation from this strategy would enable the automaker to detect and optimize the upgrade probability of its components, thereby pushing the detection rate above 48%. Consequently, the attacker's optimal choice is to maintain a 2:3 random delivery ratio between 0-day and N-day exploits, achieving a stable intrusion success rate of 52%.

When both parties adopt their optimal strategies, the maximin (defender's best worst-case) and minimax (attacker's worst best-case) values of their payoffs are equal at 48%, with a saddle point existing at the same value. According to von Neumann's minimax theorem, this value corresponds to the game's equilibrium strategy. That is, the attacker randomly delivers 0-day and N-day exploits at a 2:3 ratio, while

the automaker adjusts OTA strategies to randomly push B and A defense components for the model at a 3:7 ratio, forming the mixed equilibrium solution for this scenario.

Assumption 4: The automaker's security department improve the N-day detection rate of the B defense component to 40%, as shown in Table 6.

Table 6. Detection rates of the optimized intelligent defense component

	Known vulnerabilities (N-day)	Unknown vulnerabilities (0-day)
A defense component	60%	30%
B defense component	40%	90%

Based on the above, it can be concluded that the attacker's optimal strategy is to randomly deliver 0-day and N-day exploits at a 1:3 ratio. After the technological upgrade, the automaker can achieve an overall detection rate of 52.5% by adopting a 3:5 probability ratio for updating B and A defense components. This technological advancement by the automaker has led to the formation of a new equilibrium in the game between the two parties (as shown in Figure 7). Furthermore, the following inference can be drawn:

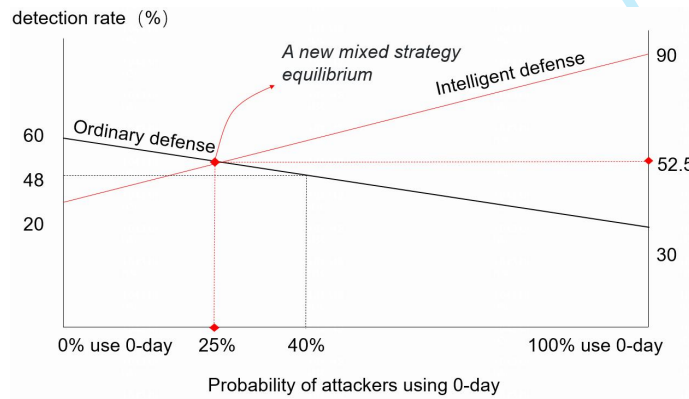


Figure 7. Mixed Strategy Outcome Analysis-3

1. The enhancement of strategic effectiveness (e.g., defense technology upgrades) not only impacts payoffs (such as increasing the defender's security benefit from 48% to 52.5%) but also alters the dynamics of the game, driving a shift from an attacker-dominant to a defender-dominant posture. Rational attackers may consequently reduce their willingness to target the system.
2. The defender's implementation and high-profile announcement of advanced defensive technologies can further influence the opponent's strategy, affecting their judgment and effectively reducing the intensity of attacks (e.g., lowering the attacker's deployment ratio of 0-day exploits from 40% to 25%).

5 Summary and Outlook

5.1 Research Conclusions

This work investigates behavioral modeling and situational evolution within the Dual-S security framework of the IoV, as well as between internal and external attackers, from a game-theoretic perspective. In resource-constrained IoV defense scenarios, local absolute security does not equate to system security, and excessive pursuit of local security may compromise or even sacrifice overall system security. The study emphasizes that functional safety and cybersecurity in IoV must establish a collaborative game relationship characterized by "Systematic collaboration," modeled as the "Dual-S Alliance." By identifying the prerequisite set for alliance formation, guiding rational resource and task allocation among heterogeneous members within the alliance, calculating marginal contributions of both parties, and dynamically adjusting strategies based on scenario-specific objectives, a stable and

sustainable cooperative solution can be established to achieve optimal system payoff.

Meanwhile, by analyzing the core contradictions in both internal and external attack-defense confrontations within the IoV, this work argues that it is unrealistic to pursue complete suppression of intruders. Instead, the optimal strategy lies in maximizing intrusion prevention with limited defensive resource, that is, seeking the Nash equilibrium in such confrontations. Through the examination of typical IoV attack-defense scenarios and the provision of methods for solving optimal strategies, this work offers a mathematical foundation to scientifically validate empirical understandings of IoV security dynamics. The findings can serve as a reference and configuration basis for optimizing security strategies and deploying scenario-specific defense within IoV security frameworks.

The IoV DNAS² framework based on the Dual-S theory constructed in this paper is a unified modeling and decision-making framework for IoV security. This study does not propose any new equilibrium concept, and future research can further explore the integration and expansion of new equilibrium theories within this framework.

5.2 Future Outlook

1. Refining the quantitative basis for payoff and other indicators

In IoV game systems, payoff computation encompasses both in-vehicle and external metrics. In-vehicle metrics include quantitative and comprehensive assessments of multi-domain contributions (e.g., Cockpit Domain, Powertrain Domain, Body Domain, chassis Domain, and ADAS Domain) to functional safety and cybersecurity, as well as unified quantification of attack-defense costs, risks, depreciation, and other indicators in specific confrontations. However, real-world scenarios are influenced by subjective factors in defining protection object values, loss measurement, and cost-risk assessment, making it impractical to use absolute values in the model for precise measurement. Future works should focus on establishing and improving industry standards for IoV security, building integrated vehicle-road-cloud risk assessment systems, and using relative rather than absolute values in game calculations to develop more scientific, multi-dimensional weighted evaluation methods. The model proposed in this paper is currently at the stage of theoretical verification and numerical illustration, and subsequent research will conduct empirical studies incorporating specific quantitative indicators based on simulation platforms such as Veins/SUMO and the IoV testbed.

2. Advancing toward evolutionary game theory

The rapid advancement of communication technologies, coupled with the deep integration of cloud computing, big data, the Internet of Things (IoT), and vehicles, is poised to infinitely expand the game space for IoV attack and defense. Evolutionary Game Theory (EGT), with its assumptions of bounded rationality, dynamic strategy adjustment, and population selection pressure, aligns more closely with the anticipated evolutionary trajectory of future game dynamics.

In cooperative games, automakers' cost pressures prevent perfect rational investments in safety and security, necessitating progressive Dual-S configuration adjustments. The wide adoption of OTA and similar techniques enables real-time, targeted threat-driven defense strategy updates, allowing players to iteratively refine strategies based on payoffs. Additionally, industry benchmarking, exploration, and market selection provide foundations for Dual-S strategy imitation, innovation, and population selection. In the future, technologies such as "Pseudonymous Certificates" and "phased upgrade and verification" that survive adjustment and adaptation will reach equilibrium under evolutionarily stable strategies and guide the alliance toward new usable fitness metrics.

In non-cooperative games, the attacker and the defender exhibit dynamic co-evolution traits. With AI and emergent intelligence empowering both sides and the expanding IoV battlefield, fully rational global optimization becomes impractical. Trial and error, imitation, and learning from experience have become mainstream strategies, more often, we build IoV cyber ranges to simulate attack-defense strategy interactions and observe the spread or elimination of strategies within groups. Multi-group games will emerge through white-hat crowdsourced testing and bounty hunters, while industry drills and penetration testing will validate strategies. Autonomous driving safety, brand image, market choices, and attack incidents will accelerate the spread of IoV threat intelligence, quantum encryption chips, and high-dimensional composite strategies. Future analysis will focus on multi-stage evolutionary game

modeling, identifying critical conditions for strategy diffusion and evolutionarily stable strategies.

3. Promoting the Practical Implementation of the Framework

Given the feasible implementation pathway of the DNAS² framework, future research will establish collaborative channels for application transformation with designers of IoV security system architectures, regulatory compliance authorities, as well as terminal and vehicle manufacturers. Designers of security system architectures can leverage the unified modeling logic of this framework to define the participants and constraint conditions of the Dual-S security system, solve for resource allocation ratios and the priority of collaborative strategies, and further guide the module division and parameter configuration of security architectures. Regulatory authorities can adopt this framework as a quantitative evaluation tool, incorporate indicators such as the functional safety failure probability of known components and the interception rate of cybersecurity components, solve for equilibria and set compliance thresholds, thus formulating a standardized Dual-S security evaluation process. Terminal and vehicle manufacturers can utilize this framework to simulate and deduce game results under different scenarios, optimize combination schemes (e.g., hardware security chips and software intrusion detection systems), design OTA dynamic update mechanisms, and maximize defensive effectiveness throughout the production and operation phases. In the future, first, we will collaborate with the aforementioned industrial partners to promote the integration of this framework into the IoV security evaluation toolchain, and gradually transform theoretical achievements into practical applications through simulation verification and engineering pilots. Second, we will expand the framework's application scenarios, for instance, optimizing the framework to adapt to complex scenarios such as heterogeneous vehicle networks. Third, we will further integrate technologies including multi-agent reinforcement learning to optimize game decision-making, thereby enhancing the integrity and engineering value of the model.

Acknowledgments

This work was supported in part by the Key Research and Development Program of Anhui Province under Grant [202103a05020007]. The authors would like to express sincere gratitude to Prof. YU Nenghai from USTC for his invaluable guidance and continuous support throughout this research. We are also deeply thankful to Dr. LIU Lin for the insightful discussions on game-theoretic modeling, and to Mr. LI Mingchun for his technical assistance with the simulation experiments.

Furthermore, we acknowledge the use of the Vehicular Network Testbed of Jiangxi Digital Internet Security Technology Co., Ltd. IoV Security Laboratory and thank the editors and anonymous reviewers for their constructive comments, which have significantly strengthened the quality and clarity of this manuscript. We particularly thank our industry partners at Jiangxi Digital Internet Security Technology Co., Ltd. for their practical perspectives on the Dual-S security requirements, which helped shape the problem formulation. Additionally, early feedback from members of the H3C IoV Security Lab on the DNAS² framework architecture is gratefully acknowledged.

Funding

This work was supported by the Key Research and Development Program of Anhui Province (Project: *5G Edge Computing Technology and Application Demonstrations for Autonomous Driving*) under Grant 202103a05020007.

Conflicts of interest

The authors declare no competing interests.

Data availability statement

No data are associated with this article.

Author contribution statement

- SUN Songer: Conceptualization, Supervision, Funding Acquisition, Resources, Writing – Review & Editing.
- YU Nenghai: Conceptualization, Methodology, Review.
- LIANG Liwen: Formal Analysis, Methodology, Investigation, writing – Original Draft, Writing – Review & Editing.

References

[1] Zhai S, Qian B H, Wang R, Wei Z B. An overview of the development and application of connected vehicle technologies[C]//24th

- International Conference on Computer, Communication, Signal Processing and Software Technology (CCSSTA). 2023: 1-8. <https://doi.org/10.26914/c.cnkihy.2023.053715>.
- [2] Song L Y, Luo X, Deng L L. Analysis on the development status and construction mode of the internet of vehicles[J]. Journal of Library and Information Science, 2021, 6(3): 45-52.
- [3] Gollmann K A, Newton M A H. Cybersecurity for connected and autonomous vehicles: A survey[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(3): 1234-1245. <https://doi.org/10.1109/TITS.2020.3006589>.
- [4] Koopman P, Ferrell U, Fratrick F, Wagner M. A safety standard approach for fully autonomous vehicles[C]//Romanovsky A, Troubitsyna E, Gashi I, Schoitsch E. Computer Safety, Reliability, and Security. Berlin: Springer, 2019: 326-332. https://doi.org/10.1007/978-3-030-26248-2_21.
- [5] Shah S A A, Newton M A H. A survey on security and privacy issues in connected vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 21(4): 1567-1578. <https://doi.org/10.1109/TITS.2019.2918581>.
- [6] ISO/SAE 26262-2018, Road vehicles—Functional safety[S]. Geneva: International Organization for Standardization (ISO); Warrendale: Society of Automotive Engineers (SAE International), 2018.
- [7] 2025 global automotive and smart mobility cybersecurity report.[R]. <https://upstream.auto/reports/global-automotive-cybersecurity-report>.
- [8] Qu X H. Analysis and research on network security risks of internet of vehicles[J]. Intelligent Building & Smart City, 2025, (10): 178-183. <https://doi.org/10.13655/j.cnki.ibci.2025.10.059>.
- [9] Xu Y J, Wu J H, Gong Y X. A brief analysis of cybersecurity in the internet of vehicles[C]//China Computer Federation. Proceedings of the 39th National Conference on Computer Security. Shanghai: ShanghaiTech University Press, 2024: 141-145. <https://doi.org/10.26914/c.cnkihy.2024.043746>.
- [10] Zhou J H, Hou Y Z, Lü C C, et al. A review on security and defense technologies for intelligent connected vehicle[J]. J Wuhan Univ (Nat Sci Ed), 2023, 69(5): 617-635. <https://doi.org/10.14188/j.1671-8836.2022.0191>.
- [11] Ren K, Yang K, Shen H T, et al. A survey of cybersecurity for intelligent connected vehicles[J]. Journal of Cybersecurity, 2024, 2(6): 89-102. <https://doi.org/10.20172/j.issn.2097-3136.240602>.
- [12] Ge C, Zhou H Y. A comprehensive security framework for intelligent and connected vehicles[J]. Intelligent Connected Vehicles, 2021, (6): 35-42. <https://doi.org/10.28896/n.cnki.nxnqc.2021.000242>.
- [13] Sun Z M. The research on joint optimization method of quality of service and security in vehicular networks based on game theory[D]. Master Thesis. Jilin: Jilin University, 2022. <https://doi.org/10.27162/d.cnki.gjlin.2022.000263>.
- [14] Feng Y. Research on performance optimization technology of connected vehicle network based on game theory[D]. Master Thesis. Xi'an: University of Electronic Science and Technology of China, 2023. <https://doi.org/10.27005/d.cnki.gdzku.2023.002713>.
- [15] Zhejiang Jin Yichang Technology Co., Ltd. A time resource allocation method for internet of vehicles system based on game theory[P]. China Patent: CN117042151A, 2023-11-07.
- [16] Ku Y K, Zhuang H Y, Wang C X, et al. Stackelberg-game-based intelligence vehicle decision method for merging scenarios[J]. Journal of Shanghai Jiao Tong University, 2022, 56(8): 987-995. <https://doi.org/10.16183/j.cnki.jsjtu.2020.319>.
- [17] Kanzow C, Facchinei F. Generalized Nash equilibrium problems[J]. Annals of Operations Research, 2010, 175(1): 173-210. <https://doi.org/10.1007/s10479-009-0667-5>.
- [18] Başar T, Olsder G J. Dynamic noncooperative game theory[M]. 2nd ed. Philadelphia: Society for Industrial and Applied Mathematics (SIAM), 1999.
- [19] ISO/SAE 21434-2021, Road vehicles—Cybersecurity engineering[S]. Geneva: ISO; Warrendale: SAE International, 2021.
- [20] UNECE. UN Regulation No. 155: Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system[S]. Geneva: United Nations Economic Commission for Europe, 2021.
- [21] UNECE. UN Regulation No. 156: Uniform provisions concerning the approval of vehicles with regards to software update and software update management system[S]. Geneva: UNECE, 2021.
- [22] SAC. GB 44495-2024, Technical requirements for vehicle information security[S]. Beijing: Standards Press of China, 2024.
- [23] SAC. GB 44496-2024, General technical requirements for vehicle software upgrade[S]. Beijing: Standards Press of China, 2024.



SUN Songer is the Senior Vice President of H3C Technologies Co., Ltd. (H3C) and the President of its subsidiary, H3C Information Security Technology Co., Ltd., His research interests include cybersecurity and data security, as well as vehicle networking security.



YU Nenghai is a professor at the University of Science and Technology of China (USTC), with primary research interests in information security.



LIANG Liwen is the Director of H3C Security Lab, with research focus on cybersecurity offense and defense, and vehicle networking security.