Misbehavior Detection in Connected Vehicle: Pre-Bayesian Majority Game Framework

Adil Attiaoui, Mouna Elmachkour, Abdellatif Kobbane, Marwane Ayaida

Misbehavior Detection in Connected Vehicle: Pre-Bayesian Majority Game Framework

Adil Attiaoui[1,3][a], Mouna Elmachkour[2], Abdellatif Kobbane[1][b] and Marwane Ayaida[3][c]
[1]*ENSIAS, Mohammed V University in Rabat, Morocco*
[2]*FSJES-SALE, Mohammed V University in Rabat, Morocco*
[3]*Polytechnique Hauts-de-France, CNRS, Univ. Lille, UMR 8520 - IEMN, F-59313 Valenciennes, France*

Keywords: Misbehavior Detection, Connected Vehicles, Bayesian Games, Majority Game, Vehicular Ad Hoc Networks, Trust Mechanisms, Collaborative Decision-Making, Ephemeral Networks.

Abstract: Ephemeral networks, such as vehicular ad hoc networks, face significant security challenges due to their transient nature and susceptibility to malicious nodes. Traditional trust mechanisms often struggle with dynamic topologies and short-lived interactions, particularly when adversarial nodes spread misinformation. This paper proposes a dual-game theoretical framework combining pre-Bayesian belief updates with majority voting to enhance collaborative misbehavior detection in decentralized vehicular networks. The approach models node interactions through two sequential games: a pre-Bayesian game where nodes assess information credibility based on individual beliefs, followed by a majority game that aggregates collective decisions to refine trust evaluations. Simulations across scenarios with varying malicious node proportions demonstrate the framework's adaptability, showing consistent belief convergence toward accurate classifications despite increased adversarial influence. Results indicate robust performance even when 40% of nodes exhibit malicious behavior, though convergence delays highlight challenges in highly adversarial environments. The study underscores the importance of maintaining benign node majorities for system stability and suggests future integrations with machine learning for scalability. This work provides a foundation for secure, real-time decision-making in applications requiring reliable ephemeral networks, such as connected vehicle systems.

1 INTRODUCTION

The rapid expansion of peer-to-peer communication between wireless devices has led to the emergence of ephemeral networks, characterized by their transient nature due to the unpredictable presence of mobile nodes. These networks, which are prevalent in applications such as vehicular ad hoc networks (VANETs), mobile social networks, and wireless sensor networks, offer substantial utility but are also highly vulnerable to malicious activities. Malicious nodes can manipulate data, disseminate false information, or disrupt communication, thereby compromising network performance. For example, in VANETs, a malicious vehicle might inject false traffic information, causing significant disruptions or even accidents, while others may refuse to forward packets, undermining routing efficiency.

While connected vehicles promise enhanced road safety and improved driver experiences by reducing accidents, they also require significant investments in infrastructure and equipment to ensure reliable, real-time road perception. The accuracy and reliability of these systems depend on robust validation mechanisms capable of detecting and mitigating malicious or erroneous data. Hardware or software failures, incorrect data processing, and data reliability issues can degrade data quality, further complicating the system's ability to deliver accurate road perception.

In the absence of centrally managed oversight in these transitory networks, ensuring trust and cooperation among neighboring nodes becomes critical. However, individual nodes often exhibit selfish behavior, driven by resource constraints and uncertainties about the intentions and reliability of other participants. These uncertainties ranging from the accuracy

[a] https://orcid.org/0009-0007-9549-6692
[b] https://orcid.org/0000-0003-3593-4084
[c] https://orcid.org/0000-0003-2319-3493

Attiaoui, A., Elmachkour, M., Kobbane, A. and Ayaida, M.
Misbehavior Detection in Connected Vehicle: Pre-Bayesian Majority Game Framework.
DOI: 10.5220/0013359100003941
In *Proceedings of the 11th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2025)*, pages 529-536
ISBN: 978-989-758-745-0; ISSN: 2184-495X

of detection mechanisms to the potential value of collaboration can deter cooperation, hampering efforts to enhance security and performance(Ben Elallid et al., 2023). Various strategies have been proposed to detect and mitigate misbehavior in such networks. Comprehensive reviews, such as those in (van der Heijden et al., 2019) and (Loukas et al., 2019), highlight diverse solutions for cyber-physical systems (CPSs) and intelligent transportation systems, particularly for transient networks with unique node constraints. For example, (Liu et al., 2006) examined attacker-defender interactions in ad hoc networks, modeling scenarios where malicious nodes could attack or not while defenders alternated between monitoring and non-monitoring states. Their game-theoretic analysis provided valuable insights into optimizing independent decision-making strategies (Manshaei et al., 2013). However, this approach focused on individual agent interactions and did not address the broader challenge of identifying misbehaving nodes across an entire network.

Reputation-based systems rely on building a credit history for nodes based on their past behavior(Hendrikx et al., 2015). While effective in some contexts, they require continuous monitoring and long-term data storage, making them less suitable for ephemeral networks where connections are brief(Hendrikx et al., 2015). To address trust and reliability in vehicular networks, (Attiaoui et al., 2024) propose a reputation-based game-theoretic trust mechanism that dynamically adjusts trust matrices based on past interactions. Unlike traditional approaches, their framework penalizes malicious behavior while rewarding true contributions without requiring persistent data storage.

In other research, a local revocation process has been proposed to account for the dynamic nature of ephemeral networks (Raya et al., 2008) (Arshad et al., 2018). In this process, a benign node, acting as an initiator, is assumed to detect or suspect a malicious node. It then broadcasts the identification (ID) of the target node, marking it as an accused node. Subsequently, neighboring benign nodes participate in a local voting-based mechanism to determine whether the target node should be discredited. The authors of (Raya et al., 2008) and (Liu et al., 2010) analyzed this local revocation process as a sequential voting game, wherein a benign node can adopt one of three strategies regarding the target node: voting, abstaining, or self-sacrificing. A benign node's decision to vote or abstain is guided by economic considerations within the game. Alternatively, it may employ a self-sacrificing strategy, invalidating both its identity and that of the target node.

The author in (Liu et al., 2010) have indicated two major limitations of revocation processes in VANETs: first, assuming complete information among nodes, and second, the problem of false-positive and false-negative rates in misbehavior detection. To address these issues, (Alabdel Abass et al., 2017) introduced an evolutionary game model where benign nodes cooperate in a voting game in order to refine revocation decisions and reduce unnecessary or overly aggressive actions. Various other studies proposed weighted voting schemes in clustering architectures (Raja et al., 2015) and (Kim, 2016), and collaborative false accusation prevention(Masdari, 2016). (Naja et al., 2020) tackled the decision-making problems of VANETs by proposing a GMDP model in order to find the optimal dissemination of alert messages. Their approach minimizes redundancy and delay while maximizing message reachability, leveraging Mean Field Approximation (MFA) to take up inter-vehicle dependencies in decision making.

In (Diakonikolas and Pavlou, 2019) the authors investigated the inverse power index issue in designing weighted voting games, concluding that the problem is computationally complex for a wide range of semi-value families. In another study, (Subba et al., 2016) proposed an intrusion detection system (IDS) utilizing election leader concepts and a hybrid IDS model to reduce continuous node monitoring in mobile ad hoc networks (MANETs). They later expanded on this work in (Subba et al., 2018), incorporating a multi-layer game-theoretic approach to address challenges related to dynamic network topologies in VANETs. While these methodologies effectively reduce IDS traffic, they fail to consider the uncertainties of node behavior and the role of incentives in local voting games. Other researchers (Kerrache et al., 2018) explored the impact of incentives on misbehavior detection within UAV-assisted VANETs. The authors in (Silva et al., 2019) introduced a voting mechanism designed to generate new strategies based on existing expert-derived ones, selecting the most effective strategies while accounting for opponent models. However, this framework does not specifically address the challenge of identifying malicious nodes in ephemeral networks.

In the absence of centralized oversight, ensuring trust and cooperation among neighboring nodes in ephemeral networks becomes critical. However, individual nodes often act selfishly due to resource constraints and uncertainties about the reliability and intentions of others. Addressing these challenges requires incentive mechanisms that encourage collaboration and adapt to varying behaviors under uncertain conditions. Such mechanisms are essential to detect

malicious nodes, enhance security, and ensure the reliability and performance of ephemeral networks, particularly in critical applications like connected vehicles.

2 SYSTEM MODEL

2.1 Assumptions and Problem Description

2.1.1 Network Model

We investigate the problem of detecting misbehavior in networks where connections between nodes are short-lived, and centralized management is not available. To illustrate our approach, we use vehicular ad hoc networks (VANETs) as a typical example of ephemeral networks. In this setting, nodes, such as vehicles, are assumed to be equipped with the necessary capabilities for wireless communication. The network operates over a contention-based medium, such as IEEE 802.11p, which reflects the characteristics of wireless channel access in VANETs (Raya et al., 2008). It is also assumed that a certificate authority or similar entity has already authenticated the nodes, ensuring that each node has a unique identifier.

Within this network, we classify the nodes into two categories: malicious and benign. Malicious nodes aim to disrupt operations by spreading false information. For example, a malicious vehicle might transmit incorrect data to manipulate the behavior of a following vehicle, potentially altering the optimal distance between them (Ferdowsi et al., 2018). Benign nodes, on the other hand, are equipped with monitoring capabilities designed to detect irregularities or fraudulent signals. For example, an autonomous vehicle might use anti-spoofing techniques to identify and counteract fake GPS signals (Behfarnia and Eslami, 2018).

2.1.2 Problem Definition

The widespread adoption of connected vehicles offers the potential to significantly enhance road safety and driving experiences by reducing accidents and improving real-time road perception. However, achieving these benefits presents several challenges, particularly in ensuring accurate and reliable communication, which requires substantial investments in infrastructure and equipment. The reliability of such systems hinges on robust validation mechanisms to detect and mitigate erroneous or malicious data. Failures in hardware or software, incorrect data processing, and unreliable information can degrade data quality and compromise the system's overall performance.

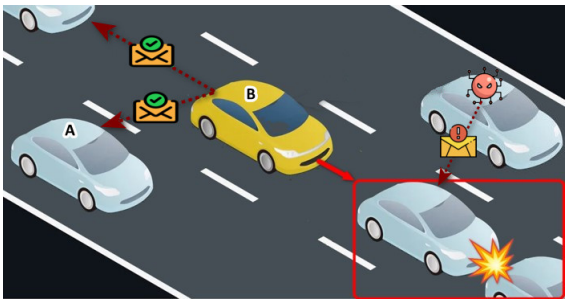

Figure 1: Security Risks in Autonomous Vehicle Networks.

In decentralized vehicular networks, where no central authority exists, vehicles (or nodes) must navigate the dual challenges of maintaining trust and collaborating effectively under uncertain conditions. For example, malicious nodes may deliberately disseminate false information to disrupt traffic or compromise safety, while benign nodes strive to preserve an accurate and truthful flow of information. This dynamic highlights the pressing need for mechanisms that enable vehicles to autonomously validate and respond to shared data in real time, even in environments characterized by fleeting connections and incomplete information.

Consider a scenario involving vehicles A and B, as illustrated in Figure 1. Suppose vehicle B detects an object on the road and aims to communicate this information to vehicle A. To do so, vehicle B sends a message to vehicle A. Upon receiving the message, vehicle A processes the data without employing any verification or trust mechanisms. This approach exposes the system to significant risks, especially in the presence of malicious actors within the network. Without robust mechanisms in place, the network becomes vulnerable to misinformation and malicious manipulation of data, to address these challenges. Such mechanisms are essential to mitigate the impact of malicious behavior and ensure the reliability of collective perception in connected vehicular networks.

2.2 Problem Formulation

2.2.1 Parameters

To model the collaborative misbehavior detection mechanism, we define the following parameters:

- **Players (Vehicles):** Represented as nodes in the network, each vehicle is classified as either *benign* (aiming to maintain safety and truthful communication) or *malicious* (seeking to spread false

information or disrupt the system).

- **Actions:** Each vehicle can choose to:
  - *Accept (A):* Trust the received information and act upon it.
  - *Reject (R):* Disregard the information as false.
- **Types:**
  - *Benign nodes* ($t = 1$)*:* Prioritize safety and correctness, aiming to propagate truthful information.
  - *Malicious nodes* ($t = 2$)*:* Seek to spread false information or obstruct correct data dissemination.
- **Belief Distribution** (p_i^t)**:** Represents the prior belief of a node i about the veracity of the received information. For example, $p_i^t = 0.75$ means the node believes the information is true with 75% confidence.
- **Information Truth** (Truth)**:** Indicates whether the information is true (Truth $= 1$) or false (Truth $= 0$).
- **Threshold** (λ)**:** A consensus parameter for the majority game, typically set as $\lambda = \lceil N/2 \rceil$, where N is the total number of vehicles.

2.2.2 Game Definition and Notations

The misbehavior detection mechanism is modeled using a *dual-game framework*:

- **First Game: Pre-Bayesian Game**
  - **Players:** N vehicles, $i \in \{1, 2, \ldots, N\}$.
  - **Actions:** Each vehicle i decides to either:
    - *Accept (A):* Trust and act on the received information.
    - *Reject (R):* Disregard the information.
  - **Utility Function:** Each vehicle's utility is defined by its type (t_i) and the veracity of the information (Truth):

$$U_i = p_i^t \cdot g(A, t_i, \text{Truth}) + (1 - p_i^t) \cdot g(R, t_i, \text{Truth}), \quad (1)$$

    where:
    - p_i^t: Belief about the information's truthfulness.
    - $g(A, t_i, \text{Truth})$: Payoff for accepting the information.
    - $g(R, t_i, \text{Truth})$: Payoff for rejecting the information.
- **Second Game: Majority Game**
  - **Set of Players:** The same set of players N is used in this game, representing the connected vehicles in the network. Each player $i \in N$ has previously made a decision in the first game (the pre-Bayesian game) and must now make a collective decision based on the choices of the other players.
  - **Set of Actions:** In this game, the actions of the players are defined as follows:
    - **Make the Majority Decision:** Each vehicle must decide to accept or reject the received information based on the majority decision from other players in the network. The majority decision is defined by a threshold $\lambda = \lceil \frac{|N|}{2} \rceil$, where $|N|$ is the total number of players (vehicles). If the majority of players accept the information, it is considered valid and accepted. If the majority rejects the information, it is considered false and rejected.
    - **Maximizing Road Safety:** Each vehicle strives to ensure that its individual decision aligns with the majority's choice to maximize road safety and improve the driving experience. The goal is to reach a consensus without requiring direct communication between the vehicles or exchange of information.
  - **Interaction Between the Games:** The link between the first game (pre-Bayesian) and the second game (majority) is established by the variable *truth*, which serves as a *pipe* between the two games. This variable determines the truthfulness of the information through the voting process. The value of *truth* (whether true or false) influences the beliefs of the players in the pre-Bayesian game, which impacts their future decisions in the majority game. In other words, learning from the first game (via belief adjustment p_i^t) influences the actions in the second game, thereby enhancing the collective decision-making dynamics.
  - **Utility Function of the Second Game:** The utility in this second game depends on the outcome of the majority vote:
    - If the majority accepts the information, this can be interpreted as an indication that the information is likely true (Truth $= 1$).
    - If the majority rejects the information, it may indicate that the information is likely false (Truth $= 0$).

    The utility of player i in this game can be modeled by a Bernoulli function, which adjusts the utility based on the majority vote result:

$$U_i' = U_i + \Delta U_i, \quad (2)$$

    where ΔU_i represents the adjustment in utility

based on the alignment of player i's decision with the majority's choice.
Thus, each vehicle adjusts its beliefs about the truthfulness of the received information based on the collective decisions of the other vehicles. This process helps to reinforce trust in the information and improves the safety and effectiveness of the decisions made in a connected driving environment.

2.2.3 Payoff Design

The payoff for each player is determined based on its action, type, and the truthfulness of the information:

- For a Benign Node ($t = 1$):
  - $g(A, 1, \text{Truth} = 1)$: High payoff if the node accepts true information, as it promotes safety (e.g., $g(A, 1, 1) = 20$).
  - $g(R, 1, \text{Truth} = 1)$: Negative payoff if the node rejects true information, potentially causing accidents (e.g., $g(R, 1, 1) = -5$).
  - $g(A, 1, \text{Truth} = 0)$: Negative payoff for accepting false information, leading to false alarms (e.g., $g(A, 1, 0) = -10$).
  - $g(R, 1, \text{Truth} = 0)$: High payoff for rejecting false information, maintaining safety (e.g., $g(R, 1, 0) = 25$).
- For a Malicious Node ($t = 2$):
  - $g(A, 2, \text{Truth} = 1)$: Negative payoff if the node accepts true information, as it fails to disrupt the system (e.g., $g(A, 2, 1) = -10$).
  - $g(R, 2, \text{Truth} = 1)$: Positive payoff for rejecting true information, partially achieving its goal (e.g., $g(R, 2, 1) = 5$).
  - $g(A, 2, \text{Truth} = 0)$: Positive payoff for accepting false information, spreading confusion (e.g., $g(A, 2, 0) = 15$).
  - $g(R, 2, \text{Truth} = 0)$: Neutral or negative payoff for rejecting false information, as it fails to disrupt (e.g., $g(R, 2, 0) = -5$).

The payoff structure ensures that benign nodes prioritize accuracy and safety, while malicious nodes aim to disrupt the system.

3 SIMULATION RESULTS

To thoroughly evaluate the proposed Cooperative Bayesian Q-Learning model with Ex-Post Validation, we conducted extensive simulations under various scenarios. Each simulation was designed to test the model's performance, resilience, and adaptability under different levels of adversarial influence.

3.1 Simulation Setup

The simulation environment consists of 23 nodes interacting over 300 iterations. Among these nodes, Player 23 is designated as an Honest node. This player is used as a benchmark to observe the evolution of its belief regarding the honesty or maliciousness of other players.

- **Belief Tracking:**
  - The red line in our results illustrates Player 23's belief about malicious nodes.
  - The green line shows its belief about honest nodes.

3.2 Malicious Node Scenarios

To simulate varying levels of adversarial behavior, we explored four distinct scenarios, each with a different percentage of malicious nodes:

- **Scenario 1:** 10% malicious nodes
- **Scenario 2:** 25% malicious nodes
- **Scenario 3:** 35% malicious nodes
- **Scenario 4:** 40% malicious nodes

Each scenario progressively increases the proportion of malicious nodes, enabling us to analyze how the model responds to greater levels of adversarial influence.

3.3 Tools and Framework

The simulations were implemented in MATLAB, leveraging its robust computational and visualization capabilities to perform Q-Learning, belief updates, and coalition management. The experiments were repeated to ensure consistency in results, and each setup adhered to the following conditions:

- **Belief Initialization:** Beliefs are initialized randomly while ensuring each node has accurate self-knowledge.
- **Action Space:** Nodes choose between two actions accept or reject messages based on updated probabilities derived from Q-values.
- **Coalition Dynamics:** Nodes with beliefs falling below a threshold of 30% are excluded from the coalition, and their interactions are halted.

This systematic approach ensures a comprehensive evaluation of the proposed model across diverse settings, providing insights into its behavior under increasing levels of malicious activity.

The numerical results depicted in Figures 2, 3, 4, and 5 provide a detailed understanding of how Player 23's beliefs evolve under varying levels of malicious node presence (10%, 25%, 35%, and 40%) across iterations.

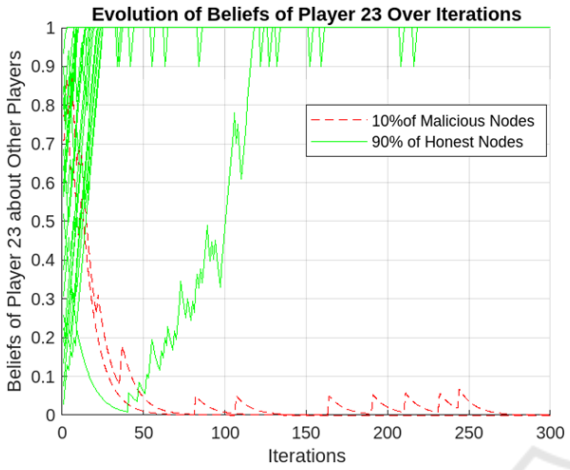

Figure 2: Case 1: Evolution of Player 23's Beliefs Over Iterations with 10% Malicious Nodes.

In Figure 2, where the network contains 10% malicious nodes, Player 23's beliefs converge quickly to stable and accurate values. The small proportion of malicious nodes ensures that benign nodes dominate the network, allowing the collaborative detection mechanism to efficiently filter out false information. This scenario demonstrates the system's robustness in environments with low adversarial influence, where trust and cooperation among nodes remain relatively unchallenged.

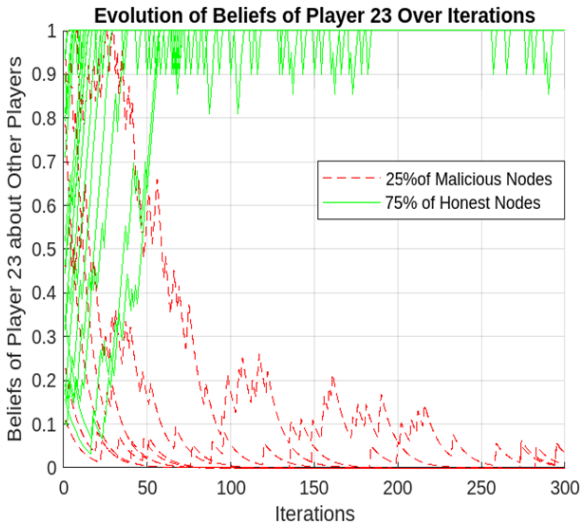

Figure 3: Case 2: Evolution of Player 23's Beliefs Over Iterations with 25% Malicious Nodes.

In Figure 3, with 25% malicious nodes, the convergence process is slightly slower compared to the 10% case. The increased presence of malicious nodes introduces more conflicting information, which delays the belief adjustment process. However, the proposed mechanism successfully enables Player 23 to identify malicious behavior and align its beliefs with the truth over time.

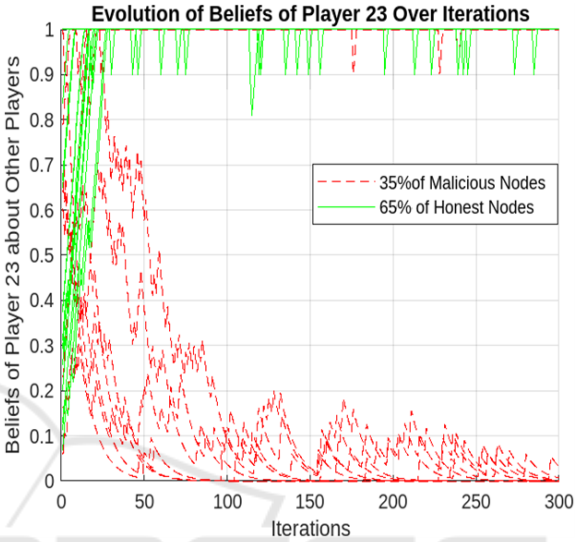

Figure 4: Case 3: Evolution of Player 23's Beliefs Over Iterations with 35% Malicious Nodes.

In Figure 4, where 35% of the nodes are malicious, the challenges posed by a higher proportion of adversaries are evident. The belief evolution displays noticeable fluctuations in the initial iterations, reflecting the increased noise and uncertainty introduced by malicious nodes. However, the slower convergence indicates the growing difficulty of maintaining trust as adversarial influence increases.

Finally, Figure 5 illustrates the most adversarial scenario, with 40% malicious nodes. Here, Player 23 experiences significant belief fluctuations in the early stages due to the near-critical threshold of malicious node influence. The high proportion of malicious nodes undermines the network's ability to achieve consensus, making belief updates more challenging. Nevertheless, the framework continues to enable gradual convergence toward accurate beliefs, albeit with reduced efficiency.

In summary, the results demonstrate that as the percentage of malicious nodes increases, the belief convergence process becomes slower and more susceptible to fluctuations. However, the framework consistently enables Player 23 to adapt and refine its beliefs, even in highly adversarial scenarios. The critical threshold around 40% malicious nodes empha-

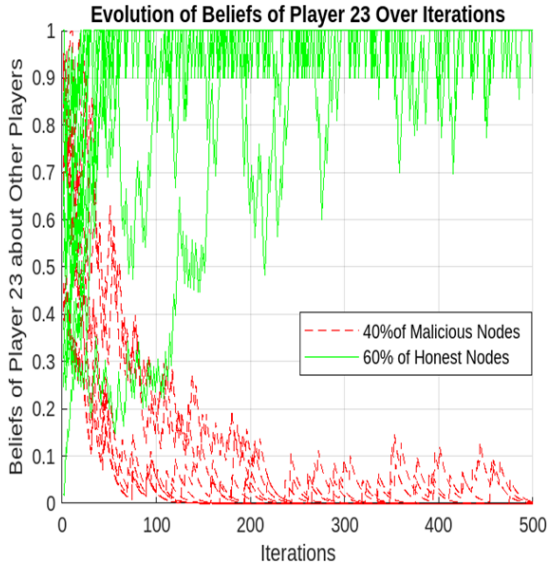

Figure 5: Case 4: Evolution of Player 23's Beliefs Over Iterations with 40% Malicious Nodes.

sizes the importance of preserving a majority of benign nodes to ensure the system's effectiveness and stability. These findings validate the robustness of the proposed framework while identifying opportunities for further optimization in high-adversarial environments.

4 CONCLUSIONS

The paper presents a misbehavior detection framework for connected vehicular networks, leveraging a dual-game approach that combines a pre-Bayesian game and a majority decision-making game. The proposed method addresses critical challenges in decentralized, ephemeral networks by enabling nodes to collaboratively and autonomously validate information in the presence of adversarial activities. Through a carefully designed belief update mechanism and reputation-based trust models, the framework ensures the reliability of shared data while mitigating the impact of malicious nodes.

Numerical simulations under varying proportions of malicious nodes (10%, 25%, 35%, and 40%) highlight the framework's robustness and adaptability. Results demonstrate that the belief evolution process is influenced by the percentage of adversarial nodes, with slower convergence and more pronounced fluctuations observed in higher-adversarial scenarios. Despite these challenges, the proposed system maintains its effectiveness, achieving accurate and reliable belief stabilization even when 40% of nodes exhibit malicious behavior.

These findings validate the potential of the proposed framework to enhance security and decision-making in connected vehicular networks. However, future work is needed to optimize the framework for scenarios with extremely high adversarial influence and to evaluate its scalability in larger, more complex networks. Additionally, integrating advanced machine learning techniques and real-world vehicular datasets could further improve the system's performance and adaptability in diverse operational environments.

ACKNOWLEDGEMENTS

This research was supported by the CNRST as part of the PhD-ASsociate Scholarship – PASS program.

REFERENCES

Alabdel Abass, A. A., Mandayam, N. B., and Gajic, Z. (2017). An evolutionary game model for threat revocation in ephemeral networks. In *2017 51st Annual Conference on Information Sciences and Systems (CISS)*, pages 1–5.

Arshad, M., Ullah, Z., Ahmad, N., Khalid, M., Criuckshank, H., and Cao, Y. (2018). A survey of local/cooperative-based malicious information detection techniques in vanets. *EURASIP Journal on Wireless Communications and Networking*, 2018.

Attiaoui, A., Elmachkour, M., Ayaida, M., and Kobbane, A. (2024). Strategic trust: Reputation-based mechanisms for mitigating malicious behavior in vehicular collective perception. In *2024 16th International Conference on Communication Software and Networks (ICCSN)*, pages 137–141.

Behfarnia, A. and Eslami, A. (2018). Risk assessment of autonomous vehicles using bayesian defense graphs. In *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, pages 1–5.

Ben Elallid, B., Abouaomar, A., Benamar, N., and Kobbane, A. (2023). Vehicles control: Collision avoidance using federated deep reinforcement learning. In *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, pages 4369–4374.

Diakonikolas, I. and Pavlou, C. (2019). On the complexity of the inverse semivalue problem for weighted voting games. *Proceedings of the AAAI Conference on Artificial Intelligence*, 33(01):1869–1876.

Ferdowsi, A., Challita, U., Saad, W., and Mandayam, N. B. (2018). Robust deep reinforcement learning for security and safety in autonomous vehicle systems. In *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pages 307–312.

Hendrikx, F., Bubendorfer, K., and Chard, R. (2015). Reputation systems: A survey and taxonomy. *Journal of Parallel and Distributed Computing*, 75:184–197.

Kerrache, C. A., Lakas, A., Lagraa, N., and Barka, E. (2018). Uav-assisted technique for the detection of malicious and selfish nodes in vanets. *Vehicular Communications*, 11:1–11.

Kim, S. (2016). Effective certificate revocation scheme based on weighted voting game approach. *IET Information Security*, 10(4):180–187.

Liu, B., Chiang, J., and Hu, Y.-C. (2010). Limits on revocation in vanets.

Liu, Y., Comaniciu, C., and Man, H. (2006). Modelling misbehaviour in ad hoc networks: a game theoretic approach for intrusion detection. *IJSN*, 1:243–254.

Loukas, G., Karapistoli, E., Panaousis, E., Sarigiannidis, P., Bezemskij, A., and Vuong, T. (2019). A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. *Ad Hoc Networks*, 84:124–147.

Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., and Hubaux, J.-P. (2013). Game theory meets network security and privacy. 45(3).

Masdari, M. (2016). Towards secure localized certificate revocation in mobile ad-hoc networks. *IETE Technical Review*, 34:1–11.

Naja, A., Oualhaj, O. A., Boulmalf, M., Essaaidi, M., and Kobbane, A. (2020). Alert message dissemination using graph-based markov decision process model in vanets. In *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pages 1–6.

Raja, K., D, A., and Ravi, V. (2015). A reliant certificate revocation of malicious nodes in manets. *Wireless Personal Communications*, 90.

Raya, M., Manshaei, M. H., Félegyhazi, M., and Hubaux, J.-P. (2008). Revocation games in ephemeral networks. In *Proceedings of the 15th ACM Conference on Computer and Communications Security*, CCS '08, page 199–210, New York, NY, USA. Association for Computing Machinery.

Silva, C., Moraes, R. O., Lelis, L. H. S., and Gal, K. (2019). Strategy generation for multiunit real-time games via voting. *IEEE Transactions on Games*, 11(4):426–435.

Subba, B., Biswas, S., and Karmakar, S. (2016). Intrusion detection in mobile ad-hoc networks: Bayesian game formulation. *Engineering Science and Technology, an International Journal*, 19(2):782–799.

Subba, B., Biswas, S., and Karmakar, S. (2018). A game theory based multi layered intrusion detection framework for vanet. *Future Generation Computer Systems*, 82:12–28.

van der Heijden, R. W., Dietzel, S., Leinmüller, T., and Kargl, F. (2019). Survey on misbehavior detection in cooperative intelligent transportation systems. *IEEE Communications Surveys & Tutorials*, 21(1):779–811.