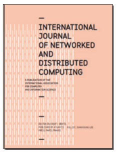
International Journal of Networked and Distributed Computing
Vol. **8**(**4**); December (2020), *pp.* 214–221
DOI: https://doi.org/10.2991/ijndc.k.200925.001; ISSN 2211-7938; eISSN 2211-7946
https://www.atlantis-press.com/journals/ijndc



INTERNATIONAL JOURNAL OF NETWORKED AND DISTRIBUTED COMPUTING

Research Article

# Secure Communications by Tit-for-Tat Strategy in Vehicular Networks

Fatima Zohra Mostefa[1,*], Zoulikha Mekkakia Maaza[1], Claude Duvallet[2]

[1] *Laboratoire SIMPA, Faculté des Mathematiques et d'Informatique Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf, USTO-MB, BP 1505, El Mnaouer, Oran 31000, Algeria*
[2] *Laboratoire LITIS, Faculté des sciences et techniques Université du Havre, Havre, France*

**ARTICLE INFO**

*Article History*

Received 18 May 2020
Accepted 09 July 2020

*Keywords*

VANET
security
malicious node
attack
game theory
Tit-for-Tat

**ABSTRACT**

Secure communication is one of the main challenges of *ad hoc* Vehicle Networks (VANET). Intrusion detection of malicious nodes is one of the solutions to secure communication in VANETs using hybrid architecture (V2V and V2I). This article proposes an approach based on game theory, in particular the "Tit-for-Tat" (TfT) strategy as a suitable paradigm for human cooperation in order to detect malicious nodes in passive and active attacks. This article analyzes the performance of the proposed approach and the "TfT" strategy contribution in VANET security.

## 1. INTRODUCTION

The Intelligent Transport System (ITS) is an important component with a new form of mobile *ad hoc* network, Vehicular *ad hoc* Networks (VANET) generate a high interest from governments, universities and private sectors. The communications transiting by a vehicle network and the information on vehicles and their drivers have to be protected and secured in order to guarantee the correct functioning of a ITS. The sensitivity of data conveyed by a VANET network reveals a high need of security. Indeed, the importance of security in this context is crucial given the critical consequences of a violation, misbehavior or an attack. Furthermore, in a very dynamic environment characterized by a nearly instant arrivals and departures of vehicles, the deployment of a security solution has to face constraints and specific configurations. Game theory is a modern branch of intelligent optimization it has been widely applied to model the behavior in a variety of applications.

This article is organized as follows. Section 2 presents security requirements. In Section 3, we describe in the current literature to secure VANET against different attacks and their detection mechanisms. In Section 4, we will present our proposed approach. In Section 5, some results obtained through simulations in Network Simulator 2 (NS2) are presented. Finally, we conclude in Section 6 and present some perspectives.

## 2. SECURITY REQUIREMENT IN VANET

Security requirements need to minimize attacks and challenges. Security requirements related to data are mainly [1]:

- Authentication: helps identifying valid entities, ensure that entities are who they claim to be, and prevent malicious parties from modifying messages.
- Confidentiality: ensures that only authorized entities can read the exchanged messages.
- Non-repudiation: ensures that a vehicle at the origin of a given information cannot be denying that it has sending it.
- Forgery: vehicles forge their own messages and transmit fake information to other vehicles.
- Resistance against tampering: timely detection of the compromise of sensitive information stored in vehicles is a very hard task. Hence, vehicles must be equipped with tamper resistant modules allowing such task.
- Data verification and integrity: in order to be able to trust exchanged messages by being sure that they were not modified from the sender to the receiver, VANET should prevent attackers from altering messages and/or detect any unauthorized modification.

In Hasrouny et al. [2], the authors classified the attackers in different parameters:

- Insider vs. Outsider: Insider is an authenticated vehicle while the outsider is an attacker who is not authenticated.

[*] *Corresponding author. Email: fatimazohra.mostefa@univ-usto.dz*

- Malicious vs. Rational: a malicious attacker searches for vulnerabilities and exploits them to disturb the system.
- Intentioned vs. Involuntary.
- Local vs. Extended: Local attackers have a specific scope of their attack range even if they compromise several entities; while extended attackers have several entities that are extended across the network.
- Active vs. Passive: Active attack creates new packets or damage existing packets in the network while passive attack snoop the wireless communication.

Different security requirements were identified in the literature. In Ahmed and Elhadef [3] the authors classify the attacks in five different criteria's:

- Attack that uses ID in order to start to steal, forge or duplicate the ID of authentic nodes.
- Attack that depend on sending false or modified messages and information.
- Attack about delaying or dropping packets or sends them to different destination.
- Attack that intercepts and/or collects information in the medium channel.
- Attack that corrupts VANET system.

As part of our research, we apply the proposed approach to these two types of attacks, active attack (Black hole attack) and passive attack (Jellyfish attack). In Black hole attack, the attacker sends data packets to its unintended destination or may drop packets. The Black hole is the area where the network traffic is rerouted [3]. In jellyfish attack, the attack maintains compliance with both the control and data protocols to make its detection and prevention difficult [4].

## 3. BACKGROUND

This paper presents some works to secure VANET against passive and active attacks. Time stamping method can be used to detect timing and replay attack (active attack). Indeed, a vehicle that receives a message checks the timestamps. If the difference between current and received timestamps is larger than a predefined threshold, the message is rejected or dropped. The main point of detection of the attack is ensuring timestamp integrity [5]. In Manvi and Tangade [6], the authors proposed to secure communication, the authentication schemes in VANET based in cryptography techniques, digital signatures and message verification techniques. However, the use of techniques such as cryptography does not offer the possibility of detecting new attacks or even of having a defense against compromised internal vehicles. In Mejri and Ben-Othman [7], authors proposed an algorithm to detect greedy behavior using a statistical method, linear regression, and watchdog software. Authors define the decision rules based in fuzzy rule, they classified the behavior of vehicles in one of the three classes: Normal, Suspected and Greedy. They began to suspect the existence of a greedy behavior from a certain value of the parameter (first threshold). Reaching a certain value of the parameter (second threshold) make suspicion high enough. Between these two threshold values, suspicion is gradual. Their idea is based on the use of the tools provided by the fuzzy logic theory which help to solve this kind of problems. Eavesdropping (passive attack) and tracking (active attack) are prevented by hiding the real and/or linking multiple authentication messages to the same vehicle by using anonymous keys exchange, pseudonyms, and group signatures [8].

Another researches based on Trust models that are used to detect malicious vehicles through the maintaining of reputations. However, due to the characteristics of VANTEs (no energy constraints, high speed, predefined movement trajectory, no centralized infrastructure...), classical trust model cannot be used as they are. Hence, maintaining reputations is very difficult even unfeasible since vehicles are moving quickly preventing them from establishing trust relations or storing reputations. Several researchers were interested then, by proposing trust environments for VANETs, [1]. In Kerrache et al. [9], authors proposed a new solution for the detection of intelligent malicious behaviors based on the adaptive detection threshold. Their solution incite attackers to behave well since any malicious behavior will be immediately detected thanks to the adaptive detection threshold. In Hasrouny et al. [10], authors proposed a security risk assessment methodology and they applied it to their Trust model. This methodology is used for identifying threats, assessing the risk involved. In Soleymani et al. [11], the proposed trust model accessed the accuracy and integrity of a sender of the event message by performing fuzzy logic. In Pham and Yeo [12], authors proposed a secure framework for vehicles to manage both trust and privacy and helped vehicles to make accurate decisions towards the data and maintain their privacy in a supple manner. The proposed approach combined both Adaptive Linkability and Recognition Scheme (ALRS) and Adaptive Trust Management Scheme (ATMS). They used three lists to classify a trust level into three lists (friendListen, neutralListen and evilListen) according to thresholds $TH_{friend}$ and $TH_{evil}$. In Ahmed et al. [13], presented a new security aware routing technique called VANSec based on a trust management approach. In fact, a decision making block checks the similarity index between the received alerts. In VANSEC, trust value falls below threshold then the node is considered as malicious.

Nowadays, blockchain-based decentralized trust management system for VANETs is merging and seems to be the new trend in such context [14].

Other researches based on game theory to secure the communication of VANETs. In Bonaci and Bushnell [15], authors used Nash Equilibrium (NE) to choose the appropriate parameters for detecting and responding to the attack. In Kamhouna et al. [16], the authors used three NEs to model trust in network to cooperate and reach the efficient equilibrium. In Ab Ghani and Tanaka [17], the authors presented a new networks game. They had considered various conditions for computing mixed NE for this game to model networks security problems whose nodes are exposed to infection by attackers. In Clark and Poovendran [18], used NEs for the simultaneous move game. In Chia and Chuang [19], authors used NE to allocate resources in each Battlefields (example phishing site in term on domain name or IP address or site on shared hosting service. In Kushwah and Sonker [20], the authors used self-organizing map classifier for the detection of misbehavior node. In this classification, they used Dempster–Shafer theory for finding attacker node is applied. In Mejri et al. [21], the Nash equilibrium of the game is obtained when the attacker vehicle continues to attack and the honest vehicle change its direction.

In Bahamou et al. [22], the authors applied attack tree- defense tree for advanced vulnerabilities assessment and intrusion detection, game theory is implemented to analyze all the potential threats that could be executed by the attacker and the possible strategies of the defender to defend the system. Also the Nash Equilibrium concept is used to define the stability state of the system, in order to build a strong defence mechanisms. Attack-tree leads the optimal intrusion detection and attack response. In Mehdi et al. [23], authors proposed a model based on an attacker and defender security game to identify and counter the attacker/malicious nodes. They also applied Nash equilibrium to calculate the best strategy for attacker and defender vehicles. The attacker initially acts like a normal node and then suddenly attacks. The strategy of the defender node is to detect and defer an attack. In their experiment, the defender node counters an attack by continuously calculating the trust level.

However, techniques that use Nash equilibrium require some computing time to find the best strategy for the attacker and defender.

Various proposals in the recent works adopted trust management as an alternative solution for it is less costly in terms of computation delay and mobility adaptation, compared to the cryptography-based solutions. Game theory based approach was introduced to use minimum resources of attacker and defender nodes compared to trust management model. Game theory analysis, help us to capture the cooperative and non-cooperative behavior of different components of a VANET system. Thus we can design the appropriate security architecture that provide incentives for individual components to contribute in the defense. Where, by using game theory, we can provide an important equilibrium that converges to the optimal possible solution.

Table 1 summarizes the studied solutions with the corresponding applied model.

Our motivation is to model the number of attempts to quickly consider a node as malicious. The use of the “Tit-for-Tat” (TfT) strategy of game theory as a mathematical model, offers a better strategy and which does not require significant computation time. The goal of our proposal is rapid decision making in order to detect and isolate malicious nodes, more specifically compromised internal nodes which are difficult to detect compared to external malicious nodes.

## 4. PROPOSED APPROACH

Security is a delicate situation; the problem is to know how to define the threshold to detect malicious nodes rapidly. In other words, the number of suspect behaviors of a node to consider it as malicious. The proposed approach relies on the use of games theory, “TfT” strategy in particular, with a rapid decision-making in order to isolate the malicious nodes. The initial idea of games theory is based on the prisoner’s dilemma in Table 2.

The prisoner’s dilemma game represents the situation of two criminals caught by the police at the same time. These criminals have two strategies to independently select from. They can either confess (defect) or not (cooperate). The results of the possible outcome are outlasted in Table 2 where:

- Two is to be prisoned for 2 years.
- Five is to be prisoned for 5 years.
- Nine is to be prisoned for 9 years.
- Zero is to be set free.

Initially Alice and Bob decided to cooperate. In Table 2, we can see (cooperate, cooperate) = (2, 2) is an optimal equilibrium but behavior’s of Alice change her strategy in goal to be free also Bob change his strategy to be free. The selfish behavior of each other results the both of participants (defect, defect). The best strategy for a criminal when both criminals do not know the other’s decision is to “defect” to avoid 9 years which is the worst case.

**Table 2** | Prisoner’s dilemma payoff matrix

| | | BOB | |
|---|---|---|---|
| ALICE | | Cooperate | Defect |
| | Cooperate | 2, 2 | 9, 0 |
| | Defect | 0, 9 | 5, 5 |

**Table 1** | Studied solutions and their model based

| Proposed solution | Model based | Methods applied |
|---|---|---|
| [10] | Trust model with group leader GL | Security risk assessment methodology |
| [11] | Fuzzy trust model | Fuzzy logic |
| [12] | Trust management | ALRS and ATMS |
| [13] | Trust management | VANSec |
| [14] | Blockchain-based decentralized trust management | Asymmetric cryptography, signature |
| [15] | Game theory | NE is used to choose the appropriate parameters for detecting and responding to the attack |
| [16] | Game theory | Three NEs are used to model trust in network to cooperate and reach the efficient equilibrium |
| [17] | Game theory | NE is used to model networks security problems |
| [18] | Game theory | NEs are used to model the simultaneous move game |
| [19] | Game theory | NE is used to allocate resources in each Battlefields |
| [20] | Game theory | Dempster–Shafer theory is used for finding attacker node |
| [21] | Game theory | NE is obtained when the attacker vehicle continues to attack and the honest vehicle change its direction |
| [22] | Game theory | NE is used to define stability of the system |
| [23] | Game theory | NE is used to calculate best strategy for attacker and defender |

In Table 2, (defect, defect) = (5, 5) is a Nash equilibrium but it is not an optimal equilibrium.

## 4.1. Nash Equilibrium Definition

Nash equilibrium is equilibrium where no participant has any incentive to change their strategy. In different games, each game we can found one or different value(s) about Nash equilibrium or no value about Nash equilibrium.

## 4.2. Classification of Game Theoretic Techniques

A game can be chosen to be cooperative or non-cooperative game according to the attack type and the expected penalty. In [24], the authors presented a comparative study of game theoretic approaches to mitigate network layer attacks in VANETs. Classification of game theoretic techniques is illustrated in Figure 1.

In VANET, a repeated game is presented targeting a defense against Blackhole attack and jelly fish attack.

### *4.2.1. Repeated game*

A repeated game is a game include different sub games in which two players repeated playing the game. This repeated game can be classified into two types:

- Finite repeated game that has a fixed period.
- Infinite repeated games played in infinite number of times.

The strategy in repeated game is called Trigger strategy. In Trigger strategy we can found:

- "Grim Trigger strategy" is suitable in investment game.
- 'TfT strategy" played in the prisoner's dilemma game.

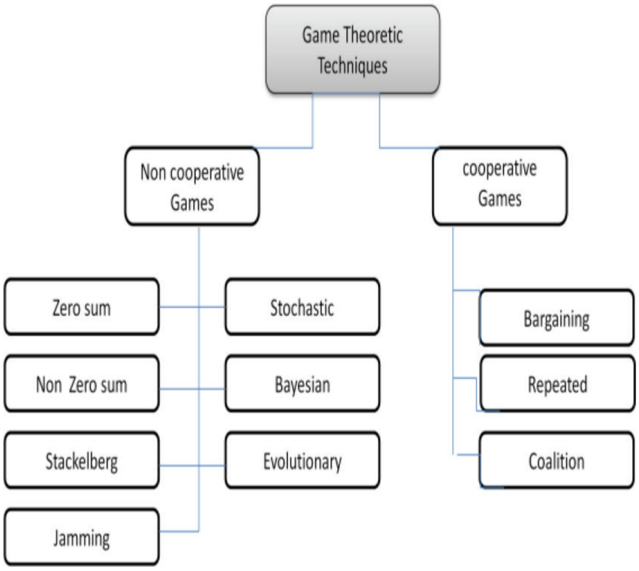


**Figure 1** Classification of game theoretic.

1. Grim Trigger strategy idea:
   - Begin to cooperate.
   - Cooperate as long as the opponent cooperates.
   - After cheating, always cheating.
2. TfT strategy idea:
   - Begin to cooperate.
   - Cooperate as long as the opponent cooperates in the previous round.
   - Cheating if the opponent cheated in the previous round.

If we compare the both strategies, Grim Trigger is harsh in punishment and lacks in credibility.

A modified version of the prisoner's dilemma game to the iterated game has been introduced in the literature. By repeating the game in several times, a player can learn the behavior of the other player. In example of Table 2, in iterated prisoner's dilemma game result always only Nash equilibrium (defect, defect) that it is not rational in reality.

Axelrod has organized tournaments between strategies. The strategies were submitted by different researchers and played different games against other strategies. Robert Axelrod has presented a winning strategy called "TfT" for repeated prisoner dilemma games in different rounds [25].

In Madhumidha et al. [26], various case studies proved that Nash equilibrium does not yield an optimal solution for repeated games.

Optimality depends on the environment. When information is complete and the payoffs are all common knowledge, defect is the only equilibrium outcome, but in practically, some information is incomplete, cooperation becomes more credible.

"Tit-for-Tat" is robust at any given environment, and that is its advantage [27].

The Nash equilibrium used in recent works is not optimal and is not suitable for repeated games with incomplete information.

By choosing the infinite repeated game whose attacker does not know the end of the game, incites the malicious nodes to adopt a good behavior in order to avoid punishment. In the case of finite game, the attacker knows the end of the game and it can cheat a second time at the end of the game in order to avoid a punishment.

By applying the "TfT" strategy in infinite repeated games in our proposed approach, we can predict behavior's of malicious nodes in the long term in order to easily detect them and isolate them from the rest of VANET.

**Tit -for-Tat strategy algorithm**

Tit-for-Tat strategy in the repeated prisoner's dilemma game is the following [28]:

- Cooperate in round 1
- For every round $k > 1$, play what the opponent played in round $k - 1$.

The idea of using "TfT" strategy is the following: to be kind, to punish, and to forgive. Firstly, TfT forces cooperation, to cheat each time generate a punishment.

In the proposed approach, we consider cheating as an attack (black hole, jellyfish attack, etc.). The punishment is withdrawal of malicious node from the neighbor tables of its neighbors and from all routing tables. The vehicles use white, Grey and black lists while Road-Side Unit (RSU) uses only grey and black lists. We consider that in the infinite repeated dilemma of the prisoner game, a game with two players (participants), the first one is the node which observes and detects the malicious node and the second one is the malicious node. Therefore, an observation is classified as either a detected **Cooperate ("C")** or a detected **Attacks ("A")** or **Decline ("D")**.

- **Cooperate ("C")** means that a node makes itself available for communication.
- **Decline ("D")** means that a node simply rejects participation.
- The malicious node **attacks ("A")** in an effort to disrupt the operation of the network that mean cheating.

We took inspiration from TfT strategy using by detection node (a node which detects a malicious node) in order to predict the incorrect behaviors and fill all malicious nodes in a Grey list then a black list and finally deciding to isolate the malicious node from the network, the idea is liked a football game. The filling of the corresponding lists by the detection node is presented in Algorithm 1.

**In first time of game:** However in first time of game, a detection node cannot distinguish whether a failure in communication caused by its opponent's "D" or "A", a detection node will be put this node in the Grey list.

**In second time of game:** if the same node cheats for the second time, detection node observe by its opponent's "A" and will be put in the black list. The nodes put in the black list are officially considered as malicious nodes. They will be removed from the routing tables.

```
Initially all neighbor nodes are in the white list;
  If a malicious node cheats in first time
    Begin
      Neighbor node of malicious node detect;
      Remove malicious node from white list;
      Put malicious node in grey list;
    end;
  If a malicious node cheats in second time
    Begin
      Neighbor node of malicious node detect;
      Remove malicious node from grey list;
      Put malicious node in black list;
    end.
```

**Algorithm 1** | The filling of the corresponding lists algorithm.

## 4.3. V2V Communication of Proposed Approach

If a node cheats for the first time, it will be put in the Grey list and if the same node cheats for the second time, it will be put in the black list. The nodes put in the black list are officially considered as malicious nodes. They will be removed from the routing tables. In what follows we present the algorithm to fill three lists (white, Grey and black).

The V2V communication to detect and isolate a malicious node uses the periodic packet "HELLO" in order to inform the vehicles about malicious nodes. In the HELLO packet, we add two fields: the field corresponds to the malicious address and the field corresponds to the malicious node degree (Table 3). The node which detects the malicious node sends the HELLO packet to his neighbors in order to inform them about the malicious node and its degree (W: white, G: Grey, B: black) to help the other nodes to update their lists while receiving the "HELLO" packet. Every node broadcasts the HELLO packet with the updated information.

In what follows we present an approach description.

Figure 2a and 2b represent the first decision about malicious node (Node 3) by putting it in the gray list. Figure 2c and 2d, represent a confirmation of the detection of the malicious node by putting it in a blacklist and isolate it from the network (deleting its entry in the routing tables).

## 4.4. V2I Communication of Proposed Approach

V2I communication (V2I and I2V), to inform the RSU and other vehicles about malicious nodes, uses the periodic "Beacon" packet containing the list of malicious nodes. We add two fields in Beacon packet (field corresponds of malicious address and field corresponds of degree of malicious node) (Tables 4 and 5).

In V2I communication, we use Beacon packet to inform RSU about malicious nodes and his degree to help RSU to update his lists when receiving Beacon packet. RSUs exchange this information with each other. In I2V communication, we use beacon packet to inform vehicles about malicious nodes and his degree to help other vehicles to update their lists when receiving beacon packet.

# 5. SIMULATION AND RESULTS

To evaluate our approach, we relied on the NS-2 simulator [29]. We use SUMO [30], to create mobility traces. In this section, we study the effects of detect Black hole attack and Jellyfish in particular Jellyfish-delay attack. Our approach detect malicious node in passive attack and active attack. Table 6 presents some simulation parameters.

**Table 3** | Some value fields in the format of Hello packet in V2V

| Source: @vehicle who detect malicious node | Destination: @ Broadcast | @malicious node | Degree (W or G or B) |
|---|---|---|---|

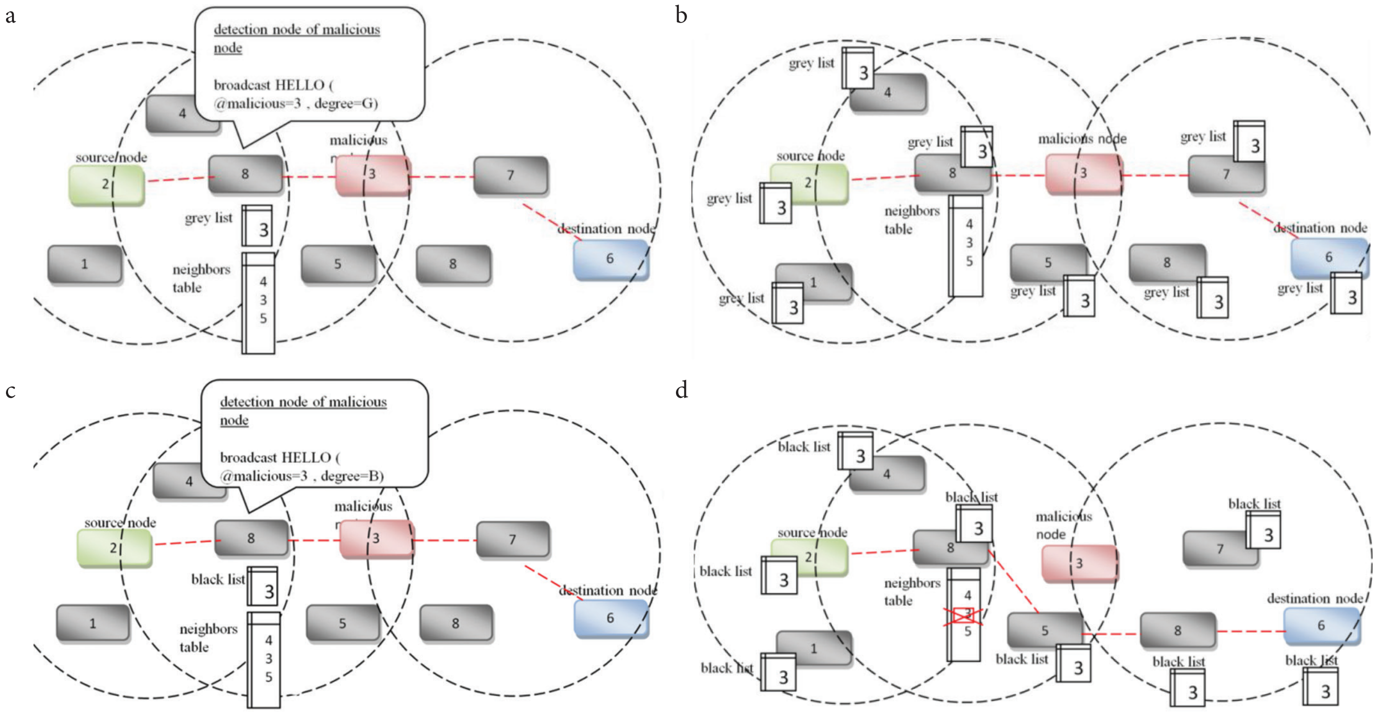


**Figure 2** | Proposed approach description in V2V.

**Table 4** | Some value fields in the format of Beacon packet (V2I)

| | | | |
|---|---|---|---|
| Source: @vehicle | Destination: @RSU | @malicious | Degree (G or B) |

**Table 5** | Some value fields in the format of Beacon packet (I2V)

| | | | |
|---|---|---|---|
| Source: @RSU | Destination: @Broadcast | @malicious | Degree (G or B) |

**Table 6** | Parameters of simulation

| Parameters | Values |
|---|---|
| Number of nodes | 10, 20, 30, 40 |
| Times of simulation (s) | 100 |
| Number of source | 2 |
| Number of destination | 2 |
| Routing protocol | AODV |
| Traffic | CBR, FTP |
| MAC | 802.11p |
| Node speeds (km/h) | 70 |

## 5.1. Active Attack (Blackhole Attack Scenario)

Black hole attracts the data packets by falsely advertising a fresh route to the destination. The proposed approach detects the malicious node in a fraction of a second, informs the other nodes, eliminates the malicious node from the routing tables and establishes a new path to the destination.

Figure 3 represents the normalized routing load. We notice that the normalized routing load rate is zero in a topology from 10 to 40 nodes with classic AODV protocol. On the other hand, in the proposed solution, the normalized routing load varies from 0.026 for a 10 nodes topology to 0.089 for a 40 nodes topology. This increase is due to the activation of the route discovering mechanism while detecting the malicious node and isolating it. Yet, it remains minimal.

## 5.2. Passive Attack (Jellyfish Attack Scenario)

Jelly Fish attack have three variants, namely [4]:

- Jellyfish reordering attack: an attacker node reorders some of the packets before forwarding them.
- Jellyfish periodic dropping attack: In this attack, nodes randomly discard some packets over a specified period during communication process.
- Jellyfish delay variance attack: round trip time of data packets vary considerably, by delaying packets randomly.

By applying jellyfish-delay attack scenario, Figure 3 represents the average end-to-end delay without and with proposed solution. In the classic case (without solution), the average end-to-end delay is 351.82 ms against 294 447 ms (with proposed solution) for a topology of 20 nodes. The malicious node intercepts the flow and delays the transmission toward the destination. This implies a high average end-to-end delay (Figure 4). With proposed solution, the average end-to-end delay was reduced, the detection node detects the malicious node, informs the neighbors and the malicious node will be isolated. A new path will be initiated to route the flow as soon as possible.

The proposed solution offers a better performance in terms of average end-to-end delay.

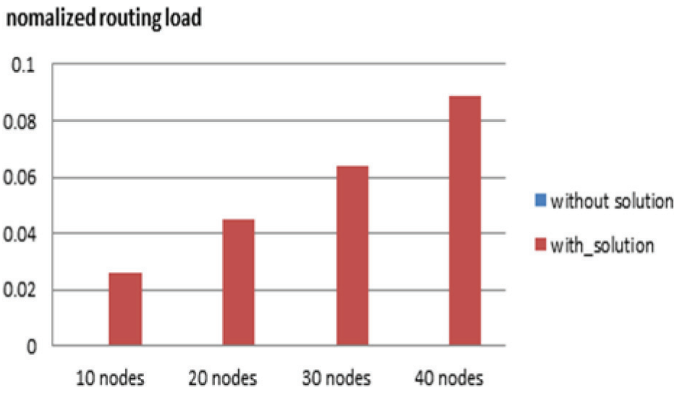


**Figure 3** | Normalized routing load.

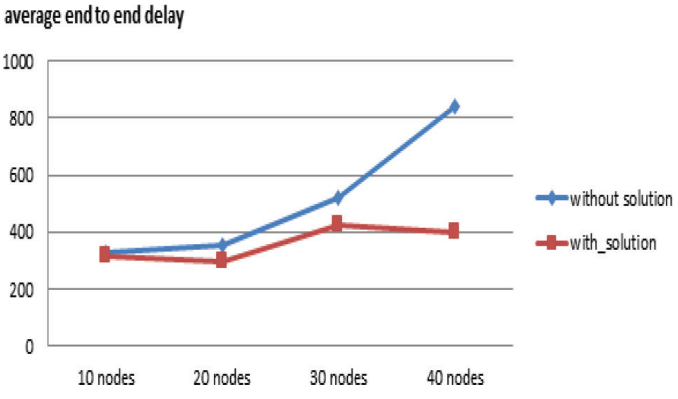


**Figure 4** | Average end-to-end delay.

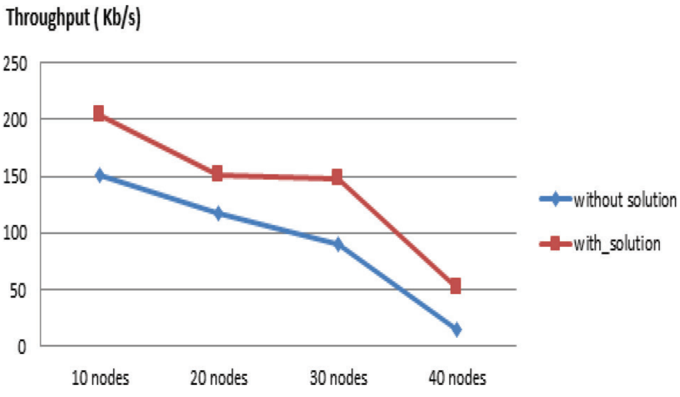


**Figure 5** | Throughput.

Figure 5 presents the network throughput with the proposed solution and the classical case according to the network density.

We notice, in a topology of 20 nodes, without proposed solution, the network throughput is 117.72 Kb/s and with proposed solution the throughput on the network is 150.83 Kb/s. We observe that the network throughput calculated according to the density is better with the proposed solution.

## 6. CONCLUSION

In this work, we have presented a secure communication approach in VANET networks using a game theory strategy called "TfT". The proposed approach allows rapid detection of attacks. We tested the approach on examples of active and passive attack in V2V mode. In V2I communication, the proposed approach also improves the process of broadcasting alerts in real time. The results of the simulation carried out show that the proposed approach is able to rapidly detect and isolate malicious nodes in the network. It offers better performance in terms of response time (detection and isolation). We plan to generalize our solution to the variety of existing active and passive attacks. We have a keen interest, especially for attacks related to the MAC sublayer. By using the approach based on the "TfT" strategy, we must achieve more robustness.

## CONFLICTS OF INTEREST

The authors declare they have no conflicts of interest.

## ACKNOWLEDGMENT

This research was supported by the Algerian Ministry of Higher Education and Scientific Research, General Direction of Scientific Research and Technological Development [grant number C00L07UN310220180003].

## REFERENCES

[1] R. Abassi, VANET security and forensics: challenges and opportunities, Wiley WIREs Foren. Sci. 1 (2019), e1324.

[2] H. Hasrouny, A.E. Samhat, C. Bassil, A. Laouiti, VANet security challenges and solutions: a survey, Vehicul. Commun. 7 (2017), 7–20.

[3] W. Ahmed, M. Elhadef, Securing intelligent vehicular ad hoc networks: a survey, in: J. Park, V. Loia, G. Yi, Y. Sung (Eds.), Advances in Computer Science and Ubiquitous Computing, Springer Nature, Singapore, 2018, pp. 6–14.

[4] V. Laxmi, C. Lal, M.S. Gaur, D. Mehta, JellyFish attack: analysis, detection and countermeasure in TCP-based MANET, J. Inform. Secur. Appl. 22 (2015), 99–112.

[5] F. Sakiz, S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV, Ad Hoc Netw. 61 (2017), 33–50.

[6] S.S. Manvi, S. Tangade, A survey on authentication schemes in VANETs for secured communication, Vehicul. Commun. 9 (2017), 19–30.

[7] M.N. Mejri, J. Ben-Othman, GDVAN: a new greedy behavior attack detection algorithm for VANETs, IEEE Trans. Mobile Comput. 16 (2017), 759–771.

[8] J. Kang, D. Lin, W. Jiang, E. Bertino, Highly efficient randomized authentication in VANETs, Perv. Mobile Comput. 44 (2018), 31–44.

[9] C.A. Kerrache, A. Lakas, N. Lagraa, Detection of intelligent malicious and selfish nodes in VANET using threshold adaptive control, 2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA), IEEE, Ras Al Khaimah, UAE, 2016, pp. 1–4.

[10] H. Hasrouny, C. Bassil, A.E. Samhat, A. Laouiti, Security risk analysis of a trust model for secure group leader-based communication in VANET, in: A. Laouiti, A. Qayyum, M. Mohamad Saad

(Eds.), Vehicular Ad-Hoc Networks for Smart Cities, Springer, Singapore, 2017, pp. 71–83.

[11] S.A. Soleymani, A.H. Abdullah, M. Zareei, M.H. Anisi, C. Vargas-Rosales, M.K. Khan, et al., A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing, IEEE Access 5 (2017), 15619–15629.

[12] T.N.D. Pham, C.K. Yeo, Adaptive trust and privacy management framework for vehicular networks, Vehicul. Commun. 13 (2018), 1–12.

[13] S. Ahmed, M. Ur Rehman, A. Ishtiaq, S. Khan, A. Ali, S. Begum, VANSec: attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead, J. Sens. 2018 (2018), 6576841.

[14] A. Kchaou, R. Abassi, S. Guemara, Toward a distributed trust management scheme for VANET, Proceedings of the 13th International Conference on Availability, Reliability and Security, Association for Computing Machinery, Hamburg, Germany, 2018, pp. 1–6.

[15] T. Bonaci, L. Bushnell, Node capture games: a game theoretic approach to modeling and mitigating node capture attacks, in: J.S. Baras, J. Katz, E. Altman (Eds.), Decision and Game Theory for Security, Second International Conference on Decision and Game Theory for Security (GameSEC), Springer, Berlin, Heidelberg, 2011, pp. 44–55.

[16] C.A. Kamhouna, N. Pissinou, K. Makki, Game theoretic modeling and evolution of trust in autonomous multi-hop networks: application to network security and privacy, 2011 IEEE International Conference on Communications (ICC), IEEE, Kyoto, Japan, 2011, pp. 1–6.

[17] A.T. Ab Ghani, K. Tanaka, Networks games with and without synchroneity, in: J.S. Baras, J. Katz, E. Altman (Eds.), Decision and Game Theory for Security, Second International Conference on Decision and Game Theory for Security (GameSEC), Springer, Berlin, Heidelberg, 2011, pp. 87–103.

[18] A. Clark, R. Poovendran, Maximizing influence in competitive environments: a game-theoretic approach, in: J.S. Baras, J. Katz, E. Altman (Eds.), Decision and Game Theory for Security, Second International Conference on Decision and Game Theory for Security (GameSEC), Springer, Berlin, Heidelberg, 2011, pp. 151–162.

[19] P.H. Chia, J. Chuang, Colonel blotto in the phishing war, in: J.S. Baras, J. Katz, E. Altman (Eds.), Decision and Game Theory for Security, Second International Conference on Decision and Game Theory for Security (GameSEC), Springer, Berlin, Heidelberg, 2011, pp. 201–218.

[20] N. Kushwah, A. Sonker, Malicious node detection on vehicular ad-hoc network using Dempster Shafer theory for denial of services attack, 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN), IEEE, Tehri, India, 2016, pp. 432–436.

[21] M.N. Mejri, N. Achir, M. Hamdi, A new security games based reaction algorithm against DOS attacks in VANETs, 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE, Las Vegas, NV, USA, 2016, pp. 837–840.

[22] S. Bahamou, D. El Ouadghiri, J.M. Bonnin, When game theory meets security and privacy related risk assessment of vehicular networks (VANET), J. Mobile Multimedia 12 (2017), 213–224.

[23] M.M. Mehdi, I. Raza, S.A. Hussain, A game theory based trust model for Vehicular Ad hoc Networks (VANETs), Comput. Netw. 121 (2017), 152–172.

[24] A. Ilavendhan, K. Saruladha, Comparative study of game theoretic approaches to mitigate network layer attacks in VANETs, ICT Exp. 4 (2018), 46–50.

[25] A. Rapoport, D.A. Seale, A.M. Colman, Is tit-for-tat the answer? On the conclusions drawn from Axelrod's tournaments, PLoS One 10 (2015), e0134128.

[26] K. Madhumidha, N. Vijayarangan, K. Padmanabhan, B. Satish, Probabilistic tit-for-tat strategy versus Nash equilibrium for infinitely repeated games with industrial applications, J. Game Theory 6 (2017), 53–61.

[27] E. Rasmusen, Games and information: an introduction to game theory, fourth ed., Basil Blackwell, 2005.

[28] A.R. Karlin, Y. Peres, Game theory, Alive, Licensed to AMS (ISBN-13: 978-1470419820), 2016.

[29] K. Fall, K. Varadhan, The NS manual, A Collaboration between researchers at UC Berkeley, LBL, USC/ISI, and Xerox PARC, 5373 (2011).

[30] M. Behrisch, L. Bieker, J. Erdmann, D. Krajzewicz, SUMO - simulation of urban mobility, The Third International Conference on Advances in System Simulation, IARIA, Barcelona, Spain, 2011.