Cooperation Enforcement Leveraging Evolutionary Game Theory for Vehicular Networks

Naercio Magaia
Department of Informatics
University of Sussex
Brighton, UK
n.magaia@sussex.ac.uk

Filipe Sousa
Instituto Superior Técnico,
Universidade de Lisboa
Lisbon, Portugal
filipe.c.de.sousa@tecnico.ulisboa.pt

Breno Sousa
Faculdade de Ciencias
Universidade de Lisboa
Lisbon, Portugal
bfmelo@ciencias.ulisboa.pt

Paulo Rogério Pereira
INESC INOV,
Instituto Superior Técnico,
Universidade de Lisboa, Portugal
prbp@inesc.pt

***Abstract*—This work concerns the design, testing, and comparison of approaches promoting the store-and-forwarding of messages in a Vehicular Delay-Tolerant Network (VDTN) while still making the network robust against attacks coming from ill-intentioned nodes that try to send large volumes of self-generated messages to cause congestion. Performance evaluation consisted of simulations with varying percentages of flooding and intermittent flooding attackers using the real-world road map of Salamanca on the Opportunistic Network Environment (ONE) simulator. Different performance evaluation metrics were considered, namely Message delivery ratio (MDR), latency, hop count, false positives in attacker detection, false negatives, reputation, and trust threshold. Evaluation metrics showed that the two novel approaches, designed using a reputation enforcement system that considers the previously known actions of opponents to isolate nodes that do not send messages from others, and also using concepts of Evolutionary Game Theory (EGT) to make the network adaptable to different states of the population of nodes, exceed the performance of the classic Tit-for-tat (TFT) and Tit-for-two-tats (TF2T) approaches for scenarios with or without attackers.**

***Index Terms*—Vehicular Delay-tolerant networks; Evolutionary game theory; Social dilemmas; Reputation enforcement system; Flood attacks.**

I. Introduction

VEHICULAR Delay-Tolerant Networks (VDTN) are becoming ever more relevant with the advent of new and more sophisticated communication technologies for vehicles, supported by the deployment of 5G mobile cells, and with the growth of the number of vehicles on the roads with Vehicle-to-Vehicle (V2V), supported by IEEE 802.11p [1], and Vehicle-to-Everything (V2X) communication capabilities. Many applications are leveraged through this VDTNs capabilities for both consumers at an individual level, like updates of software, maps, and points of interest, and also with community applications, such as smart cities or grids, that, to give some examples, aim to reduce pollution, traffic, energy waste, and increase road safety.

The VDTN's store-and-forward function makes it possible to extend the range of communications between vehicles, providing coverage to a larger number of users distributed over a larger area. It is therefore extremely important to design approaches that make possible a robust operation of VDTNs, especially in the presence of ill-intentioned nodes that must not be allowed to take down these network applications.

While proposing solutions for VDTNs, researchers may need to take into account [2]: vehicular networks have predictable mobility (i.e., vehicles need to follow existing paths, since they need to stay on the roads), high mobility (i.e., network topology changes frequently due to high speed), the network topology is adapted accordingly to time and place (i.e., traffic conditions will have an impact on the evolution of the network and the location of the scenario - urban or rural), range connection (i.e., as vehicles mainly exchange messages through wireless communication, they need to stay in range connection). Further, vehicular networks are different from VDTNs, because the first one needs to have an end-to-end connectivity path (e.g., dense networks), while VDTNs can store and carry messages for a while (e.g., sparse networks).

Furthermore, Pereira et al. [2] highlight some applications of VDTNs: cooperative collision avoidance, optimization of the traffic flow (e.g., road congestion prevention), data collection by sensors (e.g., the network can be monitored using sensors and create alerts of weather or road surface conditions), among others.

In this sense, security requirements are another key point when proposing solutions for vehicular networks. For example, ill-intentioned vehicles may attempt to perform various malicious actions in the network, such as spreading false information, holding and not forwarding messages (e.g., black-hole attack), and attempting to flood a network with noisy/irrelevant data packets (e.g., flooding attack).

In this paper, we propose two novel approaches based on a cooperation enforcement system by reputation and on EGT concepts to counteract the effects of ill-intentioned nodes that flood the network with messages while still promoting cooperation between well-intentioned nodes. Our proposed models allow nodes to adapt to changing network conditions and harmonise the interest of each node for its own gain with the overall gain for the network as a whole, which is possible by encouraging cooperation.

The structure of the paper is as follows. Section II presents the related work. Section III presents the Game Theory model for the store-and-forward mechanism and two EGT approaches. In Section IV, we discuss the attacks considered. In Section V, we present the simulation model and results. Finally, Section VI presents concluding remarks.

II. Related work

Game Theory (GT) and Evolutionary Game Theory (EGT) have been used to address different network-based aspects where researchers aim to provide better results. Tian et al. [3] used EGT to evaluate the Internet of Vehicles (IoV) reputation management scheme, where they aimed to find the most appropriate solution for fraud in connected vehicles. They also simulated and evaluated a dynamic and diverse attack strategy.

Since vehicular networks are diverse and have their own specificities, researchers may propose solutions that consider them. For example, with vehicle-to-infrastructure (V2I) communication, vehicles may send or request data to or from the Internet or other vehicles on the road via a roadside unit (RSU). Jia et al. [4] proposed a mobile RSU scheme using Software Defined Networking (SDN) and EGT. The proposed solution aimed to demonstrate the benefits of applying SDN in vehicular networks, and they modified the OpenFlow protocol stack to apply it to wireless vehicular networks. In addition, they evaluated their proposed protocol on the OPNET platform, considering some scenarios: without the mobile RSU and with SDN and EGT enabled. Sun et al. [5] highlighted the applications of GT in vehicular networks, considering their advantages, challenges, and alternative solutions. Mkiramweni et al. [6] reviewed the applicability of GT in UAV communication.

In order to investigate how damaging network attacks are and to highlight security issues in Vehicular Ad-hoc Networks (VANETs), researchers are trying to understand the different network layer attacks. In this sense, Ilavendhan and Saruladha [7] investigated the use of GT to mitigate network layer attacks in VANETs, where they classified the issues related to data authentication, data integrity, data confidentiality, message forgery, data non-repudiation, vehicle privacy, and service availability. Zahedi and Farzaneh [8] used EGT to build a security model for VANETs, where their strategy applies the method in each vehicle to identify attackers and defend victim vehicles.

Furthermore, Chen et al. [9] use a coalition game model with a reward scheme to promote message store-carry-and-foward in VANETs. Khan et al. [10] use an evolutionary coalition game for network access selection in 4G Long Term Evolution (LTE) networks. Banerjee et al. [11] promotes package transmissions on a Vehicular Network (VN) using an EGT-based approach modelled considering a Public Goods Game (PGG). Guo et al. [12] uses an EGT to devise an approach against malicious nodes in a Delay-Tolerant Network (DTN). Hamdoun et al. [13] use a coalition game for transmission power control for Machine To Machine (M2M) in 5G networks. Mekki et al. [1] use an EGT-based approach and Q-learning for the choice of the Internet access technology in a 4G LTE VANET. Khan et al. [14] uses clustering in a EGT model to solve message routing in VANET. Riaz and Park [15] use a EGT-based approach for power control in Non-Orthogonal Multiple Access (NOMA) uplinks in 5G networks. Wang et. al [16] use an EGT-based approach for choosing the internet access mode in VN aided with Unmanned Aerial Vehicles (UAVs). Finally, Ma et al. [17] use a weighted sum to reduce multiple objectives to a single optimization function optimized in a EGT approach to solve channel selection in 5G and 4G LTE-A networks.

Differently from the literature, our solution aims to resist flooding attacks by considering that 1) our enforcement system penalises players' selfish actions and 2) allows players to adapt to the changes in the network.

III. The proposed approaches

A. The GT model for store-and-forward mechanism

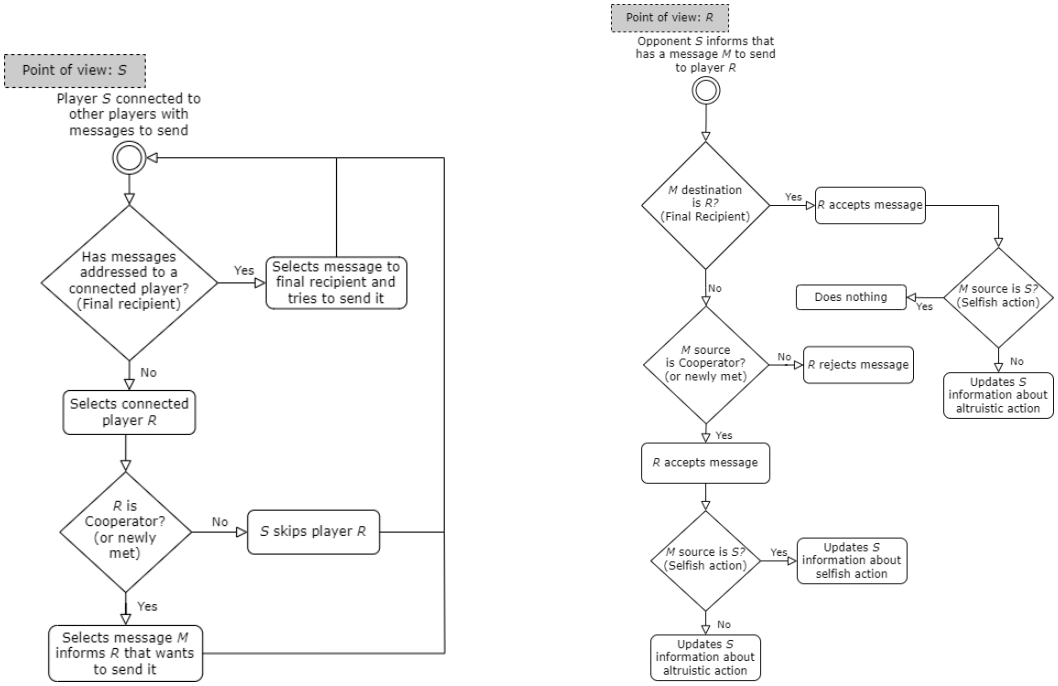
The defensive approaches tested in this work resort to a generic GT modelling. The players correspond to the network nodes, specifically vehicles in a VDTN. All players are considered to belong to the same class and they interact in pairs. Upon interaction, each player takes one of two roles: either it acts as a sender S, if it tries to send a message, or it acts as a receiver R. The decisions on whether to send a message and whether to accept a message are made according to the nature of the message and the label of the opponent. The opponents are labelled as cooperators, defectors or newly met according to the information kept by the player related to said opponents. Newly met players are treated as cooperators to promote cooperation in the beginning stages of the game.

The way the labels are assigned, and the information on the opponents is acquired and kept are the main differences between the different GT-based approaches proposed. In essence, the information on the opponents and the subsequent labels act as a reputation enforcement system since selfish actions may cause later retribution.

This game corresponds, therefore, to a Public Goods Game, where a myopic, selfish utility maximization approach without cooperation enforcement would lead to a situation where every node would become a free-rider and only direct communications would be possible. The use of reputation in detriment to a reward system is done because the decentralized nature of VDTN does not allow the existence of a centralized authority. Figs. 1a and 1b present flowcharts of the generic GT approaches for the sender S and receiver R, respectively.

Considering firstly the sender S, from the messages he has available in its transmission queue, it will give priority to messages whose targets correspond to a node that player S is connected to as these messages can be delivered directly to the final recipient. Then, the sender S will iterate through its queue until it finds a message addressed to a player previously labelled as a cooperator or newly met and will try to send it. Players labelled as defectors are discarded, as they should be isolated from the network.

From the point of view of the receiver player R, the process gets triggered when the receiver R gets informed by the sender S that it has a message to send to him. If the message is addressed to the receiver R itself, it is promptly accepted. Plus, if the message has a source different from the sender S, the sender S info is updated to inform of this last altruistic behaviour.



(a) Sender (b) Receiver

Fig. 1: Generic GT approach.

If the message is addressed to a destination other than the receiver R, the message is only accepted if the sender S was previously labelled as a cooperator or is newly met. Messages from defectors are rejected in an effort to isolate them from the network. Finally, if the message is accepted, the information of the sender S will be updated in relation to the source of the message. The action is considered selfish if the message source is the sender S itself. On the other hand, if the message was not generated by the sender S, the action is considered altruistic.

Additionally, we can formalize the strategy space for a sender S and a receiver R. The sender S can perform three different actions: *sending* its own messages S_{OM}, *forwarding* messages from other players that are holding F_M, or doing *nothing* N. On the other side of the connection, the receiver R can take two different actions: *accepting* the message A_M or *refusing* the message R_M.

$$\begin{aligned} Strat_S &= \{S_{OM}, F_M, N\} \\ Strat_R &= \{A_M, R_M\} \end{aligned} \tag{1}$$

With the previous strategy spaces and disregarding the reputation enforcement, the payoff matrix is the following:

$$S, R = \begin{bmatrix} S - C_S, -C_R & 0, 0 \\ -C_S, -C_R & 0, 0 \\ 0, 0 & 0, 0 \end{bmatrix}, S > C_S > 0, C_R > 0 \tag{2}$$

Where S is the potential gain for the player having its message stored and forwarded, C_S is the energy cost to send a message, and C_R is the energy and memory cost to receive and store a message.

As there is no previous agreement regarding the behaviour of each player, under the assumption that the players are rational, the sender will always try to send its own messages, assuming that S is greater than C_S. The receiver will always refuse messages not addressed to itself, reaching a NE where no message will be sent in the network other than direct messages.

In this situation where every node behaves as a free rider, the VDTN capability to forward messages is rendered useless. Now, when the reputation system is taken into account:

$$S, R = \begin{bmatrix} S - C_S, R_A - C_R & 0, 0 \\ R_F - C_S, R_A - C_R & 0, 0 \\ 0, 0 & 0, 0 \end{bmatrix}$$
$$, S > C_S > 0, C_R > 0, R_A > C_R > 0, R_F > C_S \tag{3}$$

where R_A is the potential gain of receiving a message that it may later forward to increase its reputation, and R_F is the gain in reputation of sending a message generated by a third party node. Now, the sender S will always try to forward messages, as long as it has already sent its own messages to the opponent in question, as long as the reputation gain value R_F is greater than the sending cost C_S. For the receiver R the message must be received as long as the value of the potential gained reputation R_A exceeds the cost C_R.

Still, one issue remains to address regarding a conflict of interests. When a sender sends a message generated by itself, this action generates a gain for himself, previously considered

S. Still, it also contributes to the congestion of the network. This approach so far does not penalize a greedy player that overflows the network resources with their own messages, a situation which leads to a dilemma similar to the "Tragedy of the Commons" [18]. To counteract this issue, an additional reputation loss for sending own messages R_S is considered, resulting in the final payoff matrix:

$$S, R = \begin{bmatrix} S - C_S - R_S, R_A - C_R & 0, 0 \\ R_F - C_S, R_A - C_R & 0, 0 \\ 0, 0 & 0, 0 \end{bmatrix} \quad (4)$$

It is important to note that selfish actions are still part of the normal VDTN behaviour. The aim of the approaches is not to extinguish selfish actions, but rather to force their coexistence with altruistic ones.

This last reputation loss mechanism for penalizing selfish behaviours will isolate flood attackers, as these ones only take selfish actions, so their poor reputations will result in a state where no opponent will cooperate with them.

B. The EGT approach

In the EGT approach, the previous actions of an opponent against the player are encoded into a ratio between its altruistic interactions and its total interactions. This ratio is the direct reputation r_d:

$$r_d = \frac{\text{Number of altruistic interactions}}{\text{Number of interactions}} \quad (5)$$

An indirect reputation metric is introduced to consider actions against other players. Upon connections, two players will communicate their list of direct reputations, here called witness.

The indirect reputation kept by P_1 of an opponent P_2 is computed as the average of the records related to that player P_2 kept in the witnesses collected so far:

$$r_{i_{P2->P1}} = Average(r_{d_{P2->Pi}}) \quad (6)$$

Where $r_{i_{P2->P1}}$ is the indirect reputation of the opponent $P2$ being computed by $P1$, $r_{d_{P2->Pi}}$ is the reputation record of the opponent P_2 witnessed by a third player P_i, and P_i is a player belonging to the set of players whom the witnesses are known by the player P_1 that includes a record for target player P_2. Finally, the effective reputation r_e is computed as a weighted sum between the direct reputation r_d and indirect reputation r_i:

$$\begin{aligned} r_e = w_d r_d + w_i r_i, \\ w_d + w_i = 1 \end{aligned} \quad (7)$$

Simplified to only take into consideration the single parameter weight of the direct reputation w_d:

$$r_e = w_d r_d + (1 - w_d) r_i \quad (8)$$

In this work, w_d is set to 0.5. As more witnesses are collected, the weight of any individual witness is diluted, making the indirect reputation metric a better indication of the actual behaviour of other players as time goes on.

We still need a way of qualifying if an opponent is labelled either as a cooperator or a defector. To do so, the effective reputation is compared against a value, called trust threshold t. The comparison works as follows:

$$\begin{cases} r_e \geq t \Rightarrow \text{opponent labelled as a cooperator} \\ r_e < t \Rightarrow \text{opponent labelled as a defector} \end{cases} \quad (9)$$

The next question is, "what should be the trust threshold value?". To answer this, we look into this threshold as a parameter that should be optimized and it is here where the evolutionary mechanism enters the scene. We consider three different objectives:

$$\begin{cases} G_O = \dfrac{N_{OAck}}{N_O} \\ G_R = \dfrac{\sum r_{ij}}{N_W} \\ C_A = 1 - \dfrac{N_A}{N_P} \end{cases} \quad (10)$$

The three objectives represent:

1) G_O - The gain of having the messages generated by the player delivered to the final recipient.
2) G_R - The average reputation of the player itself computed in the space of the witnesses collected so far. Although this metric also represents a selfish gain, in the sense that the player wants strictly for itself to have a good reputation so others will help it, the interesting characteristic of this gain is that it is also a public gain since good individual reputations lead to cooperative players and promotion of cooperation in the VDTN as a whole.
3) C_A - The cost of accepting messages. It is computed as the complement of the ratio between the messages accepted and the messages proposed so far.

The fitness function is obtained by reducing multiple objectives to a single one by weighted sum:

$$O = w_{GO} \times G_O + w_{GR} \times G_R + w_{CA} \times C_A, w_{GO} + w_{GR} + w_{GA} = 1 \quad (11)$$

We consider all the weights above to have the same value:

$$w_{GO} = w_{GR} = w_{GA} = \frac{1}{3} \quad (12)$$

Regarding the evolutionary dynamic mechanism, we consider "imitate the best". In the initial state of the population, each player randomly draws a trust threshold according to a uniform probability distribution between 0 and 1. Upon connection, the players exchange their fitness function values and corresponding trust thresholds but only after a period of maturity P_m within each generation with a period of P_g. Each player will update its trust threshold to the one that resulted in a higher payoff from the ones it knows.

C. The EGT including indirect witnesses approach

EGT with Indirect Witnesses (EGT-IW) is a variant of the EGT with a gossip mechanism added for the exchange of indirect witnesses. When two players meet, they will not only exchange their direct reputation list but also the witnesses they have collected so far.

IV. Attack Model

The misbehaving nodes are considered to attack the VDTN by performing flooding attacks, where attacking nodes generate bursts of messages addressed to other attackers until their buffer is full. After a message sent from an attacker is accepted, the attacker will drop it from its buffer. In this way, the buffer gains space for generating new attacking messages. Finally, as their main aim is not to deliver their messages to the nodes the messages are addressed to, but to cause congestion in the network, they will only send messages to receivers other than the ones the message is addressed to.

As the flood attackers, i.e., individual players that would lead to network congestion, only have an attacking behaviour, their labelling and isolation for the network should happen in the beginning stages of the attack. To further confuse the defence mechanisms, intermittent flooding attackers will switch between attacking and normal behaviours in random intermittence periods P_i, i.e., the attacker tries to raise its reputation after some time. In our simulations, we defined one hour to give time for the attacker to raise its reputation again.

V. Performance evaluation

A. The simulation model

Simulations were performed in the ONE using the real-life map of Salamanca.The radio propagation model considers the effect of interference in the data rate [19]:

$$\text{Data Rate} = \frac{\text{Data Rate}_{max}}{N_T \sqrt{N_{AT} \ln N_{AT}}} \tag{13}$$

where N_T is the number of transmissions within the transmission range, and N_{AT} is the number of active transmissions. The maximum data rate is set to 27 Mbps [20], the maximum range to 400 m [20], the simulation time to 2 days, the messages Time to Live (TTL) is set to 5 hours, the buffer size is set at 236 MB [21], and the size of the messages to vary between 500 KB and 1 MB in size. The mobility model operates as a random waypoint model, with the waypoints restricted to the points that represent in the real-world maps used by shops. Upon arriving at a selected destination, a node will wait between 0 and 5 minutes before selecting a new destination. The vehicles travel at speeds between 10 and 50 km/h. The scenarios comprehended a total of 50 vehicles. Each well-behaved node generates a message in a period between 5 and 10 minutes. The generation period P_g was set to 1 hour and the maturity period P_m to 30 mins.

Five different strategies were tested under different relative quantities of flooding attackers: (i) *Non-defensive (ND) approach*, which is based on the epidemic message routing protocol; (ii) *TFT* (tit-for-tat), where the information on the opponents corresponds directly to the label of cooperator or defector. So, the player will decide to cooperate with an opponent based solely on its last action; (iii) *TF2T (Tit-for-two-tats)*, a forgiving mechanism is introduced to counteract the tendency of TFT to sometimes too eagerly isolate nodes in the network that may not be seen as abusers when taking into consideration a bigger scope of previous actions; (iv) *EGT*, that resorts to the counting of altruists and total actions taken by opponents, to solve the issue TFT and even TF2T suffer from a lack of memory, as their information on the opponents only comprehends a maximum of two previous actions; (v) *Evolutionary Game Theory with Indirect Witnesses (EGT-IW)*, that when two players meet, exchanges not only their direct reputation list but also the witnesses they have collected so far. This additional degree of witness collection should theoretically lead to a more rapid convergence into a representative effective reputation value, consequently making the label of the attackers in the network as defectors quicker and diminishing the effects of their attacks in the early stages of the simulation, made possible by taking advantage of the initial goodwill against strangers.

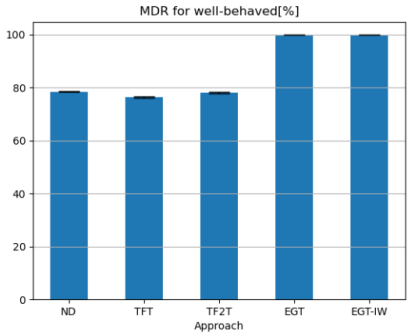
The tests were made with no attackers, 10%, 20%, 30%, 40% and 50% attackers, taking into consideration two different types of attacks, flooding attacks, and intermittent flooding attacks, and five strategies, resulting in 55 test scenarios. For each of these 55 scenarios, five different runs are performed with different seeds. Every result is therefore presented with a confidence interval of 95% under a normal probability distribution.

B. Simulation metrics and results

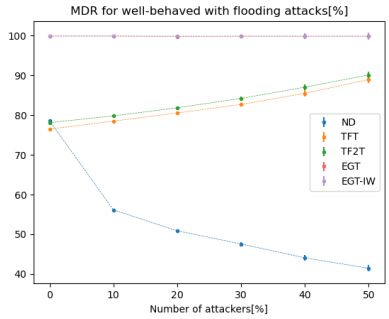
To evaluate the performance in the simulations, the following metrics were used, segregated if they referred to well-behaved or attacking nodes: (i) *Message delivery ratio (MDR)*, the ratio between the messages received and the total messages sent; (ii) *Average latency*, average latency for the messages successfully sent; (iii) *Overhead*, an indication of the amount of transmission on the network relative to the delivered messages; (iv) *False positives and negatives*, the labels of cooperator and defector are only used for the approaches that aim to isolate misbehaving nodes. Therefore, this metric does not apply to the ND approach.

We first ran our scenarios without attackers to see how damaging the proposed attacks were. The purpose of these scenarios is to test whether the defensive approaches degrade the network's operation compared to the ND approach. Then, we present the MDR, average latency, average hop count, and overhead of the attack scenarios.

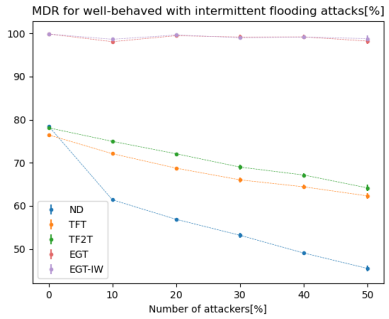
1) Message Delivery Ratio (MDR): Fig. 2 show the influence of each strategy on the MDR. For the case with no attackers (Fig. 2a), TFT and TF2T have a tiny network performance degradation. This small degradation is explained by the immediate retaliation for nodes sending their own messages, but this retaliation is marginal in the overall scenario. EGT and



(a) No Attackers

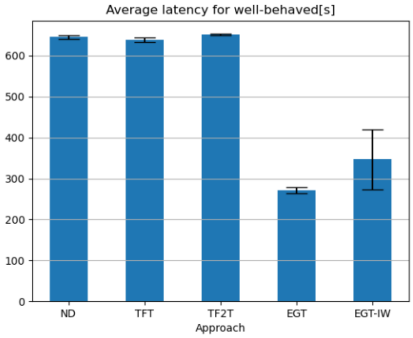


(b) flooding Attackers

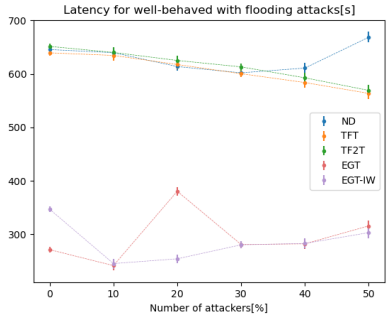


(c) Intermittent flooding Attackers

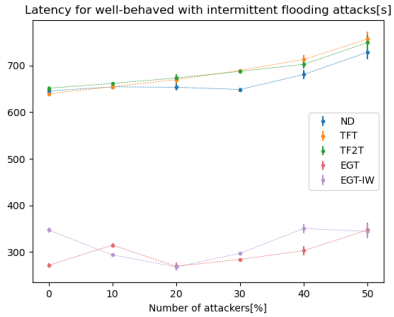
Fig. 2: MDR



(a) No Attackers



(b) flooding Attackers



(c) Intermittent flooding Attackers

Fig. 3: Latency

EGT-IW perform considerably better as the epidemic routing can lead to local congestion that is attenuated by the filtering of the EGT selective behaviour.

When the number of attackers increases, MDR degrades for ND. TFT and TF2T have some improvement with flooding attackers (Fig. 2b), but their MDR decreases with the intermittent flooding attack (Fig. 2c). Indeed, as the intermittent attackers are harder to identify, the attack is more effective. However, in both scenarios, our proposed solution can distinguish the flooding traffic more effectively than ND, TFT, and TF2T. While the difference between EGT and EGT-IW is marginal for the flooding attackers' case, EGT-IW is better for the intermittent flooding attackers' case due to the gossip mechanism.

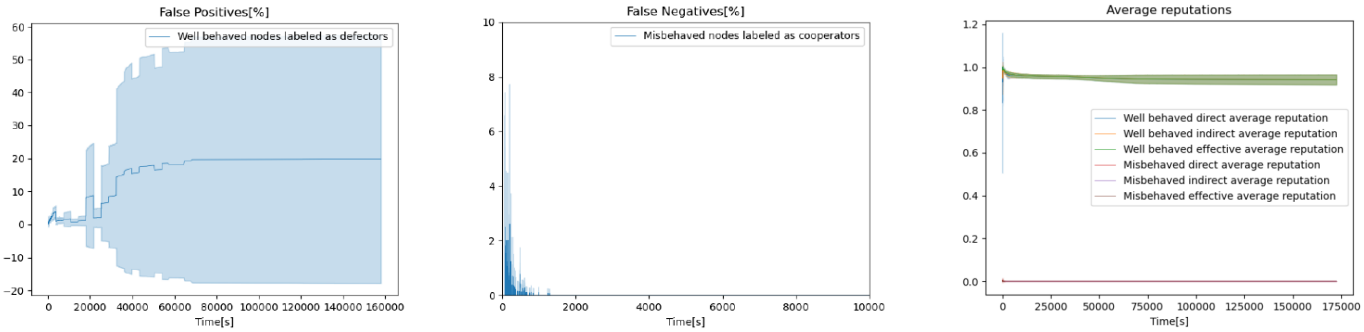
2) Average latency: Concerning the average latency, we see better performance for EGT and EGT-IW (Fig. 3) compared to the remaining approaches. However, contrary to what we see for TFT and TF2T, the latencies rise with the increasing number of attackers. The fewer well-behaved nodes can explain this; the only ones that cooperate and make the connections are the chances to forward messages, which are rarer.

3) Overhead: ND results in very low cooperation in the presence of attackers resulting in a low overhead. EGT and EGT-IW has half the overhead of TFT and TF2T with flooding attackers.

Overall, the EGT and EGT-IW approaches perform extremely well with delivery probabilities close to 100%, overheads lower than the rest of the tested approaches, and high average hop counts, indicating that cooperation is being promoted.

4) False positives and negatives: Although EGT-based approaches present a high performance on average over multiple runs, partially due to the promotion of cooperative behaviour, they may also lead to non-cooperative states when looking into some occasional individual cases.

In Fig. 4a, we can see a case where one of the five runs ends up selected for a high trust threshold value, causing a high number of false positives, seen in the graph by the long confidence interval, and the consequent state of low cooperation. This occurs in a single case because only one of the average hop counts for messages generated by well-behaved nodes is close to 1, indicating a low level of cooperation. In addition, Fig. 4b and Fig. 4c show the false negatives and average reputation, respectively, for 20% of attackers. We can see that misbehaving nodes are correctly identified very fast. EGT-IW is quicker than EGT to converge due to the gossip mechanism that allows faster convergence. TFT and TF2T are much slower. However, in some cases, good nodes may be temporarily misidentified due to the random initial state of the network.



(a) False positives (b) False negatives (c) Average reputation

Fig. 4: False positives and negatives, EGT, 20% flooding Attackers

VI. Conclusions

In this work, we proposed two models for the enforcement of cooperation in VDTNs, where we performed simulations to validate our proposed solution under flooding and intermittent flooding attacks. Furthermore, our work was mainly divided into three types of tests:

Compared to the ND approach, the TFT and TF2T leads to a marginal performance degradation. However, with the EGT and EGT-IW approaches, we can see a good performance increment.

TFT and TF2T show good performance in this case, being able to protect the network against congestion and even being able to increase its performance with the relative quantity of attackers increase. Even so, EGT and EGT-IW still got a considerably better performance against these attacks.

Although TFT and TF2T still showed a considerable degree of protection against congestion, it was less effective than in the case of flooding attacks due to the short-term memory of these approaches. Once again, EGT and EGT-IW were also shown to protect the network against this kind of attacks. Also, EGT-IW showed a performance increase when compared to EGT, demonstrating that for this case the quicker detection of defection in the network provided by the gossip mechanism leads to better overall results.

References

[1] T. M. et al., "Proactive and hybrid wireless network access strategy for Vehicle Cloud networks: An evolutionary game approach," *2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC 2017*, pp. 1108–1113, jul 2017.

[2] P. R. P. et al., "From delay-tolerant networks to vehicular delay-tolerant networks," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 1166–1182, 2011.

[3] Z. T. et al., "Evaluating Reputation Management Schemes of Internet of Vehicles Based on Evolutionary Game Theory," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 5971–5980, jun 2019.

[4] F. J. et al., "A BUS-aided RSU access scheme based on SDN and evolutionary game in the Internet of Vehicle," *International Journal of Communication Systems*, p. e3932, 2019.

[5] Z. Sun, Y. Liu, J. Wang, G. Li, C. Anil, K. Li, X. Guo, G. Sun, D. Tian, and D. Cao, "Applications of game theory in vehicular networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2660–2710, 2021.

[6] M. E. Mkiramweni, C. Yang, J. Li, and W. Zhang, "A survey of game theory in unmanned aerial vehicles communications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3386–3416, 2019.

[7] A. Ilavendhan and K. Saruladha, "Comparative study of game theoretic approaches to mitigate network layer attacks in vanets," *Ict Express*, vol. 4, no. 1, pp. 46–50, 2018.

[8] F. Zahedi and N. Farzaneh, "An evolutionary game theory–based security model in vehicular ad hoc networks," *International Journal of Communication Systems*, vol. 33, no. 6, p. e4290, 2020.

[9] T. C. et al., "Stimulating cooperation in vehicular ad hoc networks: A coalitional game theoretic approach," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 2, pp. 566–579, feb 2011.

[10] M. A. Khan and H. Tembine, "Evolutionary coalitional games in network selection," *2011 Wireless Advanced, WiAd 2011*, pp. 185–194, 2011.

[11] A. B. et al., "Cooperation Optimized Design for Information Dissemination in Vehicular Networks using Evolutionary Game Theory," *CoRR*, vol. abs/1301.1, pp. 1–15, 2013.

[12] H. Guo, X. Wang, H. Cheng, and M. Huang, "A routing defense mechanism using evolutionary game theory for Delay Tolerant Networks," *Applied Soft Computing*, vol. 38, pp. 469–476, 2016.

[13] S. Hamdoun, A. Rachedi, H. Tembine, and Y. Ghamri-Doudane, "Efficient transmission strategy selection algorithm for M2M communications: An evolutionary game approach," *Proceedings - 2016 IEEE 15th International Symposium on Network Computing and Applications, NCA 2016*, pp. 286–293, dec 2016.

[14] A. A. K. et al., "An evolutionary game theoretic approach for stable and optimized clustering in vanets," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4501–4513, may 2018.

[15] S. Riaz and U. Park, "Power control for interference mitigation by evolutionary game theory in uplink NOMA for 5G networks," *Journal of the Chinese Institute of Engineers, Transactions of the Chinese Institute of Engineers,Series A*, vol. 41, no. 1, pp. 18–25, 2018.

[16] G. W. et al., "Mode Selection in UAV-Aided Vehicular Network: An Evolutionary Game Approach," *2018 10th International Conference on Wireless Communications and Signal Processing, WCSP 2018*, nov 2018.

[17] M. Ma, A. Zhu, S. Guo, X. Wang, B. Liu, and X. Su, "Heterogeneous network selection algorithm for novel 5G services based on evolutionary game," *IET Communications*, vol. 14, no. 2, pp. 320–330, 2020.

[18] G. Hardin, "The tragedy of the commons," *Science*, vol. 162, no. 3859, pp. 1243–1248, 1968.

[19] P. Gupta and P. R. Kumar, "The Capacity of Wireless Networks," *IEEE Transactions on Information Theory*, vol. 46, no. 2, 2000.

[20] J. H. Wen and C. E. Weng, "Performance evaluation of IEEE 1609 WAVE for vehicular communications," *International Journal of Vehicular Technology*, vol. 2013, pp. 344–348, 2013.

[21] S. Pramanik and R. Datta, "Buffer Size Estimation for Nodes in Delay Tolerant Vehicular Networks under Self-Similar Traffic," *Canadian Conference on Electrical and Computer Engineering*, vol. 2018-May, aug 2018.