A Game Theoretic Approach to Analyse Security between Smart Vehicles and Parcels in Smart Cities.

El Arbi ABDELLAOUI ALAOU1,2,* and Mastapha EL MOUDDEN3,**

1EIGSI, 282 Route of the Oasis, Maarif, 20140 Casablanca, Morocco.
2E3MI Team, Department of Computer Science, FST Errachidia - Moulay Ismail University, Morocco.
3Department of Mathematics, Faculty of Sciences, Meknes - Moulay Ismail University, Morocco.

Abstract. The Internet of Things (IoT) is considered as a modern concept that will revolutionize the near future. Its interest is to create an environment of combined intelligent devices and systems, communicating with each other through wireless networks. Urban logistics are an applicative field of this new technology, especially for smart parcels and vehicles. Actually, in the context of economy development, the competitiveness between companies and territories necessarily involves an improvement of logistics services. Although these gains offered by IoT, there are significant obstacles to counter. One of the important obstacles to consider is the security. In this paper, we will analyze the interaction between selfish smart vehicles/parcels and malicious smart vehicles/parcels, that was formulated as a game model. As a result, we have calculated the Nash equilibrium and the utilities for the both selfish smart vehicles/parcels and malicious smart vehicles/parcels, evaluated the parameters that can maximize the selfish smart vehicles/parcels’s utility when the smart parcels are transported by vehicles between different centers (shops, supermarket, etc) was planned and identify the potential malicious smart vehicles/parcels.

1 Introduction

The term "Intelligent Transportation Systems (ITS) " is generally used to refer to technology, infrastructure and services of tomorrow; as well as the planning and the control methods used for the persons and freight transportation. In addition, the intelligent transport system (ITS) came as a solution to different transportation problems, such as traffic congestion; related to the world motorization, the urbanization, the population growth and the change in population density [1].

The goal of Intelligent Transportation Systems (ITS) is to integrate individual transportation elements and join them through use of information and communication technologies into a single system. ITS provide the opportunity to increase the use of existing transportation system and generate additional capacity from the existing physical infrastructure. Other benefits of freight ITS include, but not limited to, increase safety and security, decrease negative environmental impacts of freight transportation.

The core of ITS consists in obtaining, processing and distributing information for a better use of the transportation system, infrastructure and services. Indeed, as data and information transmission become increasingly shared thanks to ITS, there is a need to establish more open data/information formats, interfaces and communication protocols. Harmonization and standardization of collected and processed data, as well as the information delivered, form part of this overall ITS standardization strategy. This can be achieved through examining and identifying the internationally adopted standards or best-practices and adapting them to the local context. Another area of importance is the communication security, especially when sensitive or confidential information is being transmitted. In this era of heightened security, some measures need to be taken to ensure that overall ITS ecosystem remain robust and secured. Likewise, the importance of privacy and anonymity should not be overlooked and proper measures need to be in place to maintain data anonymity. All these will enhance users’ confidence and acceptance of ITS.

In this paper, we are exploring the applicability of game theoretic approaches to address the ITS security issues and some of these approaches look promising, such as freight transport in cities. The goal of the research is to design a solution of the security between the vehicles and parcels in smart cities using game theory. The challenge of this work is to manage the communication between the selfish and malicious smart vehicles/parcels in smart city in order to mitigate attacks based on malicious smart vehicles/parcels. We have modeled the selfish and malicious strategies using Game Theory approach in a normal form so as to find the Nash equilibrium to evaluate the benefits and costs for each strategy. We are exploring the applicability of game theoretic approach to protect the the communication between the smart vehicles and parcels in smart city [10] [9] [3]. So, the main contributions of this paper can be summarized as follows:
• to analyze of the security smart vehicle and parcel with the game theory;
• to model interaction between the selfish smart vehicles/parcels and the malicious smart vehicles/parcels in smart city;
• to determine the payoff of the selfish smart vehicles/parcels and the malicious smart vehicles/parcels;
• to characterize the Nash equilibrium (NE) of each strategy.

The rest of the paper is organized as follows. In Section 2 we describe our problematic. Then, the Section 3 provides an analysis of interactions between the selfish smart vehicles/parcels and the malicious smart vehicles/parcels, with a special focus on game theory approach in smart cities. In Section 4, we analyze the game equilibria for selfish smart vehicles/parcels and malicious smart vehicles/parcels. Finally, We conclude the paper in Section 5.

2 Problem and statement

In our study, we consider a smart city with a selfish and malicious smart parcels, and a set of smart vehicles (selfish and malicious) implicated in the inter-centers transportation process (shops, supermarket ...); and we want to know the action/interaction between the selfish and malicious smart vehicles/parcels, in order to secure the communication between them.

![Figure 1. Diagram explaining our problematic](image)

3 Game formulation

In this work, to formally analyze the security issue in smart cities, we model the dynamic interactions between the selfish smart vehicles/parcels and the malicious smart vehicles/parcels as a non-cooperative game [9] [10]. Our security non-cooperative game model is inspired by the work in [4].

The non-cooperative game model to be described has the following three components:

**Players** The set of the legitimate smart vehicles/parcels in an smart cities, which is composed of the malicious smart vehicles/parcels who is the abstraction of one or multiple smart vehicles/parcels with malicious intent to compromise the smart cities and the selfish smart vehicles/parcels defending them. \( \{ P^D_t \}_{n, j = 1}^m \) and \( \{ P^c_t \}_{m, j = 1}^m \) denote the set of the malicious smart vehicles/parcels and the selfish ones, respectively.

**Strategy space** Assume that an smart cities consisting of smart vehicles/parcels that are capable of deciding whether to collaborate with one another or defect. On the one hand, most of them are selfish and want to preserve their resource. On the other hand, they have to transport the smart parcels to the different centers in smart cities. At the same time, for some malicious smart vehicles/parcels, they may advertise false delivery information, not transport smart parcels correctly, fabricate, modify, or simply drop smart parcels, the action set of the smart vehicles/parcels is defined as follows:

\[
S = \{ C, D \}
\]

where \( C \) represents collaboration and \( D \) denotes defection. In this work, \( x(s) \) denotes the probability that selfish smart vehicles/parcels discover the malicious smart vehicles/parcels at time \( t \). For the selfish smart vehicles/parcels, the bigger \( x(s) \), the more gains they will obtain. For simplicity, the gain \( g_{mi}(x(s)) \) of the selfish smart vehicle/parcel \( P^c_{mi} \) is given as follows

\[
g_{mi}(x(s)) = g_{mi}(x(t))
\]

where \( g_{mi} \) is a positive parameter.

\( f_{m}(t) \) denotes the number of smart parcels that has been scheduled to transport and have successfully arrived at their centers of destination at time \( t \) by the selfish smart vehicle \( P^c_j \). For a collaborate smart vehicle/parcel \( P^c_{m} \)

\[
S = \{ C, D \}
\]

if a smart parcel originated from a selfish smart vehicle can be successfully delivered to its center of destination, then the smart vehicle can get gain \( g_{mi} \). For simplicity, \( r_{m}(f_{m}(t)) \) represents the smart parcels that have been scheduled to transport and have successfully arrived at their centers of destination, which is given as follows:

\[
r_{m}(f_{m}(t)) = f_{m}(t)g_{mi}
\]

where \( g_{mi} \) is a positive parameter.

\( h_{mj}(i, t) \) denotes that a smart vehicle \( P^D_j \) drops or injects the number of smart parcels, which are transported by the smart vehicle \( P^c_{m} \) at time \( t \). It is natural to assure that the smart vehicles/parcels are resource limited in smart cities, and they take into account the amount of energy spent. If the smart parcels are dropped or injected by the malicious smart vehicles and are not discovered by the selfish smart vehicles, the malicious smart vehicle can obtain gains \( w_{mj}(h_{mj}(i, t)) \). For simplicity, the gains \( w_{mj}(h_{mj}(i, t)) \) of the malicious smart vehicle \( P^D_{mj} \) is defined as follows:

\[
w_{mj}(h_{mj}(i, t)) = (1 - x(s))h_{mj}(i, t)c
\]

where \( c \) is a positive constant.

In what follows, \( u_i(s) \) denotes the resource consume rate of a smart vehicle/parcel \( i \) (i.e., amount of resources) that is devoted to securing that information at time \( s \), which is a ratio, so its unit is 1.

\[
u_i(s) = \frac{\text{resource consume at time } s}{\text{the total of smart vehicle/parcel } i}
\]
Assume that the cost paid by the selfish smart vehicle/parcel $P_{mi}$ is given as follows:

$$y_{mi}(u_{mi}(s)) = \frac{c_{mi}}{2}u_{mi}(s)^2$$

(6)

and the cost paid by the malicious smart vehicle/parcel $P_{nj}$ is defined as follows:

$$y_{nj}(u_{nj}(s)) = \frac{c_{nj}}{2}u_{nj}(s)^2$$

(7)

The selfish smart vehicles/parcels are rational, a selfish smart vehicle $P_{mi}$ seeks to maximize the instantaneous probability $x(s)$ and maximize the smart parcels $f_m(t)$ that have been scheduled to transport and have successfully arrived at the centers of destination; and minimize resource consumption incurred by their actions. Assume that the game is a perfect information game. A selfish smart vehicle/parcel $P_{mi}$ chooses the optimal amount of network resource $u_{mi}(s)$ to invest in information security contingent upon the state of game in order to maximize the individual utility function $U_{mi}$.

The utility function for the selfish smart vehicles/parcels is defined as follows:

$$U_{mi} = \int_{t_0}^{T} \left[ q_{mi}x(t) + f_{mi}(t)g_{mi} - \frac{c_{mi}}{2}u_{mi}(s)^2 \right] e^{-r(T-t_0)} ds$$

$$+ e^{-r(T-t_0)} S_{mi}x(T)$$

(8)

where $r > 0$ denotes discount factor, values received $t$ time is discounted by the factor $r$, and $S_{mi}x(T)$ denotes the marginal utility of the smart vehicle/parcel $P_{mi}$ at time $T$.

The malicious smart vehicles/parcels, unlike the selfish smart vehicles/parcels, are motivated by the reward for disrupting or jamming the transmissions of other center. Similarly, for a malicious smart vehicle/parcel $P_{nj}$, we can model the malicious smart vehicles/parcels’ utility function as follows:

$$U_{nj} = \int_{t_0}^{T} \left[ q_{nj}(1-x(s)) + (1-x(s))h_{nj}(i,s)\right] e^{-r(T-t_0)} ds$$

$$+ e^{-r(T-t_0)} S_{nj}[1-x(T)]$$

(9)

When $x(s) = 1$, the selfish smart vehicles/parcels’ instantaneous probability that discovers the malicious smart vehicles/parcels is 100 %, according to our model, the increase of $x(s)$ means increase the intensity of the defensive countermeasures to against attacks, which may cost their large amounts of resources, so the selfish smart vehicles/parcels have to decrease their intensity of the defensive countermeasures to save their resources. Similarly, assume that $x(s) = 0$, the probability that discovers the malicious smart vehicles/parcels is 0, the selfish smart vehicles/parcels don’t take any defensive countermeasure to against attacks, which may threat the network security. So the selfish smart vehicles/parcels have to increase their intensity of the defensive countermeasures to against attacks. For simplicity, the dynamics of the probability $x(s)$ that discovers malicious smart vehicles/parcels is governed by:

$$\frac{dx(s)}{ds} = \sum_{i=1}^{m} u_{mi}(s)[1-x(s)]^{1/2} - \sum_{j=1}^{n} u_{nj}(s)x(s)^{1/2}$$

$$x(0) = x_0$$

(10)

4 Nash equilibrium solutions

In the game theory, the Nash Equilibrium is an important concept. The players will meet an agreement if NE exists.

In this section, we study the node’s behavior and characterize the equilibria structure of the selfish smart vehicles/parcels and the malicious smart vehicles/parcels. In fact, none of the selfish smart vehicles/parcels and the malicious smart vehicles/parcels make a pre-agreement, so they seek a Nash equilibrium solution, $u(s)$.

4.1 Nash Equilibrium Solution for the Selfish smart vehicles/parcels

Let $u_{mi}^{(0)}(t, x) = [u_{m1}^{(0)}(t, x), u_{m2}^{(0)}(t, x),..., u_{mm}^{(0)}(t, x), u_{m1}^{(0)}(t, x), u_{m2}^{(0)}(t, x),..., u_{mm}^{(0)}(t, x)]$, for $t \in [t_0, T]$. $W^{(0)}(t, x) : [t_0, T] \times \mathbb{R}^n \rightarrow \mathbb{R}$ denotes the value function of the selfish smart vehicles/parcels $P_{mi}$.

For the selfish smart vehicles/parcels $P_{mi}$, $i \in \{1, 2, \ldots, m\}$ a feedback Nash equilibrium solution to the equations (8), (10) satisfies the following conditions:

$$-V^{(0)}_{mi}(t, x) = \max_{U_{mi}} [q_{mi}x(t) + f_{mi}(t)g_{mi} - \frac{c_{mi}}{2}u_{mi}(t)^2] e^{-r(t-t_0)}$$

$$+ \sum_{i=1}^{m} u_{mi}^{(0)}(t, x)[1-x(t)]^{1/2}$$

$$+ \sum_{j=1}^{n} u_{nj}^{(0)}(t, x)x(t)^{1/2}$$

$$- \sum_{j=1}^{n} u_{nj}^{(0)}(t, x)x(t)^{1/2}]$$

$$V^{(0)}_{mi}(t, x) = e^{-r(T-t_0)} S_{mi}x(T).$$

(11)

The Nash equilibrium solution for the selfish smart vehicles/parcels by performing the indicated maximization in equation (11) yields

$$u_{mi}^{(0)}(t, x) = \frac{V^{(0)}_{mi}(t, x)}{c_{mi}} (1-x)\frac{1}{2} e^{r(t-t_0)} \quad \text{for } i \in \{1, 2, \ldots, m\}.$$  

(12)

4.2 Nash Equilibrium solution for the malicious smart vehicles/parcels

For malicious smart vehicles/parcels $P_{nj}$, $j \in \{1, 2, \ldots, n\}$ a feedback Nash equilibrium solution to the equations (9), (10) has to satisfy the following conditions
$$-V_i^{(ih)}(t,x) = \max_{c_i} \left[ [q_i(1-x(t)) + (1-x(t))h_{nj}(t,t)c - \frac{c_i}{2}u_{nj}(t)^2]e^{-r(t-\tau)} + V^{h}_{m}(x, t) - u_{nj}(t)[x(t)]^{1/2} \right]$$

$$+ \sum_{j=1}^{n} u_{nj}(t,x)[1-x(t)]^{1/2}$$

$$- \sum_{j=1}^{n} u_{nj}(t,x)(x(t))^{1/2}]$$

$$V^{m}_{i}(t,x) = e^{-r(t-\tau)}S_{nj}(1-x), \quad (13)$$

Similarly, the Nash equilibrium solution for the malicious smart vehicles/parcels by performing the indicated maximization in equation (13) yields,

$$u_{nj}^{(ih)}(t,x) = \frac{-V_{m}(t,x)}{c_{nj}}x^{1/2}e^{r(t-\tau)} \text{ for } j \in [1, 2, \ldots, n]. \quad (14)$$

Substituting \(u_{nj}^{(ih)}(t,x)\) and \(u_{nj}^{(ih)}(t,x)\) into (11) and (13), respectively, and solving ((11) and (13), we obtain the value functions

$$V_{m}(t,x) = e^{-r(t-\tau)}[A_{mi}(t)x + B_{mi}(t), \quad \text{for } i \in [1, 2, \ldots, m], \quad (15)$$

$$V_{m}(t,x) = e^{-r(t-\tau)}[A_{nj}(t)(1-x) + B_{nj}(t), \quad \text{for } j \in [1, 2, \ldots, n]. \quad (16)$$

where \(A_{mi}(t), B_{mi}(t), A_{nj}(t), \text{ and } B_{nj}(t)\) satisfy

$$\frac{A_{mi}(t)}{dt} = rA_{mi}(t) - q_{mi} + \frac{A_{mi}^{2}(t)}{2c_{mi}} + \sum_{k=1}^{m} A_{mi}(t)A_{mk}(t)$$

$$+ \sum_{j=1}^{n} A_{nj}(t)A_{mj}(t) \quad (17)$$

$$A_{mi}(T) = S_{mi} \quad (18)$$

$$B_{mi}(t) = rB_{mi}(t) - f_{mi}q_{mi} - \sum_{j=1}^{m} A_{mj}(t)A_{mk}(t) \quad (19)$$

$$B_{mi}(T) = 0 \quad (20)$$

$$A_{nj}(t) = rA_{nj}(t) - q_{nj} - h_{nj}c + \frac{A_{nj}^{2}(t)}{2c_{nj}} + \sum_{i=1}^{m} A_{nj}(t)A_{ni}(t)$$

$$+ \sum_{j=1}^{n} A_{nj}(t)A_{mj}(t) \quad (21)$$

$$A_{nj}(T) = S_{nj} \quad (22)$$

$$B_{nj}(t) = rB_{nj}(t) - q_{nj} - h_{nj}c + \sum_{i=1}^{m} A_{mi}(t)A_{nj}(t)$$

$$= rB_{nj}(t) - q_{nj} - h_{nj}c + \sum_{i=1}^{m} A_{mi}(t)A_{nj}(t) \quad (25)$$

For the symmetric case, (17) becomes

$$A_{nj}(T) = 0. \quad (26)$$

Similarly, we have that

$$A_{nj}(t) = \frac{A_{mi}(t)}{c_{mj}}(1-x(t))^{1/2} \quad (27)$$

upon substituting the relevant partial derivatives of \(V_{m}(t,x)\) and \(V_{m}(t,x)\) from (15) and (16) into (12) and (14) yields the feedback Nash equilibrium strategies

$$u_{mi}^{(ih)}(t,x) = \frac{A_{mi}(t)}{c_{mi}}(1-x(t))^{1/2} \quad (29)$$

for the selfish smart vehicle/parcel \(P_{mi}^{C}, i \in [1, 2, \ldots, m]\)

and

$$u_{nj}^{(ih)}(t,x) = \frac{A_{nj}(t)}{c_{nj}}x(t)^{1/2} \quad (30)$$

for the selfish smart vehicle/parcel \(P_{nj}^{D}, j \in [1, 2, \ldots, n] \).

Substituting the game equilibrium strategies above into (10) yields the optimal state trajectory:

$$\frac{dx(s)}{ds} = -\left( \sum_{i=1}^{m} \frac{A_{mi}(t)}{c_{mi}} + \sum_{j=1}^{n} \frac{A_{nj}(t)}{c_{nj}} \right) x(s) + \sum_{i=1}^{m} A_{mi}(t)$$

$$x(0) = x_{0} \quad (31)$$

$$x'(t) = \omega(t_{0}, t) \left( \int_{t_{0}}^{t} \frac{A_{mi}(t)}{c_{mi}} \omega^{-1}(t_{0}, t) ds + x_{0} \right), \quad (33)$$

for \(t \in [t_{0}, T] \),

where

$$\omega(t_{0}, t) = e^{-\int_{t_{0}}^{t} H(s) ds} \quad (34)$$

and

$$H(x) = -\left( \sum_{i=1}^{m} \frac{A_{mi}(t)}{c_{mi}} + \sum_{j=1}^{n} \frac{A_{nj}(t)}{c_{nj}} \right) \quad (35)$$

The Nash equilibrium strategies, \(u_{mi}^{(ih)}(t,x)\) and \(u_{nj}^{(ih)}(t,x)\), which are strategy profile for the non-cooperative game with the property that no nodes can improve its gains by altering its strategy unilaterally while the other nodes keep their strategies unchanged [26,27].
5 Conclusion

In this paper, we have studied and analyzed the security between vehicles and parcels in smart cities by using a non-cooperative game. We have first introduced a non-cooperative game model of the interactions between vehicles and parcels in smart cities. Then, we have analyzed the set of Nash equilibrium of the game and discuss its implications for each strategy of our game and presented some necessary conditions for existence of Nash equilibrium.

References

[1] K. Abdul Khaliq, A. Qayyum and J. Pannek. "Novel Routing Framework for VANET Considering Challenges for Safety Application in City Logistics”. In Vehicular Ad-Hoc Networks for Smart Cities, Volume 548, pp. 53-67, 2017.

[2] A. Roumboutsos, S. Kapros. "A game theory approach to urban public transport integration policy.” Transport Policy, ELSEVIER, Volume 19, pp. 209–215, 2008.

[3] Abou El Majd, B., Desideri, J. A., and Habbal, A. (2010). Aerodynamic and structural optimization of a business-jet wingshape by a Nash game and an adapted split of variables. Mécanique and Industries, 11(3-4), 209-214.

[4] E. A. Abdellaoui, K. Nassiri, M. El Moudden. "Framework for Analyzing of Inter-cluster Communication in the DRHT by Using Game Theory", in The Mediterranean Symposium on Smart City Applications (SCAMS 2017), ACM, October 25-27, 2017 Tangier, Morocco.

[5] Chunli, L. "Intelligent transportation based on the Internet of things.” in IEEE 2nd International Conference on Consumer Electronics, Communications and Networks, IEEE, 2012.

[6] R. El-Azouzi, F. Pellegrini, V. Kamble. "Evolutionary forwarding games in Delay Tolerant Networks.” In proceedings of the 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), IEEE pp. 81–89, 2010.

[7] Dimitrakopoulos, G., Demestichas, P., Koutra, V." Intelligent management functionality for improving transportation efficiency by means of the car pooling concept”. In journal the IEEE Trans. Intell. Transp. Syst. pp. 424–436, 2012.

[8] Elhenawy, M., A. Elbery, A., A. Hassan, A.” An intersection game-theory-based traffic control algorithm in a connected vehicle environment.” In: IEEE 18th International Conference on Intelligent Transportation Systems, IEEE, 2015.

[9] Pan, F., Xi, B., Wang, L.: "Environmental regulation strategy analysis of local government based on evolutionary game theory," in 2014 International Conference on Management Science and Engineering (ICMSE), 2014.

[10] Wei, L., Wei, G. : "Decision-making on reverse logistics for manufacturers: an evolutionary game theory perspective". In: International Conference on Logistics, Informatics and Service Sciences (LISS), 2015.