Security analysis for intelligent urban freight transport

El Arbi Abdellaoui Alaoui*

Department of Mathematics and Computer Science,
Engineering School EIGSI-Casablanca,
282 Route of the Oasis, Casablanca, Morocco
Email: elarbi.abdellaoui@eigsica.ma
and
Department of Computer Science,
Faculty of Sciences and Technology,
Moulay Ismail University,
BP 509, Boutalamine – 52 000, Errachidia, Morocco
Email: abdellaoui.e@gmail.com
*Corresponding author

Mustapha El Moudden

Department of Mathematics and Computer Science,
Faculty of Sciences,
Moulay Ismail University,
Meknes, Morocco
Email: muelmoudden@gmail.com

Abstract: The actual evolution of the traditional transport functions resulted from to the prominent digital revolution, the emergence of the internet of things (IoT), the use of intelligent transport systems (ITS) and the development of communication technologies. In fact, the development of the internet of things (IoT) and geo-localisation contributes significantly in the actual evolution, meanwhile allowing the emergence of new mobility services such as e-commerce, carpooling, car sharing and management vehicle fleet. Hence, impacting strongly the traditional economic means. In this context, one of the important obstacles to consider is the security. In this paper, we will analyse 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, evaluate the parameters that can maximise the selfish smart vehicles/parcels' utility when the smart parcels are transported by vehicles between different centres (shops, supermarket, ...) was planned and identify the potential malicious smart vehicles/parcels.

Keywords: intelligent transport system; ITS; smart city; smart parcel; internet of things; IoT; security; smart vehicle; game theory; Nash equilibrium.

Reference to this paper should be made as follows: Abdellaoui Alaoui, E.A. and El Moudden, M. (2019) 'Security analysis for intelligent urban freight transport', *Int. J. Information Privacy, Security and Integrity*, Vol. 4, No. 1, pp.49–64.

Biographical notes: El Arbi Abdellaoui Alaoui received his PhD in Computer Science in 2017 from Faculty of Sciences and Technology – Errachidia, University of Moulay Ismaïl, Meknès, Morocco. Prior to this, he received his Master's degree in Telecommunication in 2013 from the National School of Applied Sciences, University of Sidi Mohamed Ben Abdallah, Fès, Morocco. Currently, he is a Research Professor at EIGSI Engineering School, Casablanca, Morocco. His research interests include mainly wireless networking, ad hoc networking, DTN networks, game theory, internet of things (IoT), smart cities and optimisation.

Mustapha El Moudden received his PhD in Applied Mathematics from the Faculty of Siences, Moulay Ismaïl University (Meknes, Morocco) in 2018, and his Master degree in Mathematics and Applications in Engineering Sciences in 2013. He has a number of publications in the field of non-differentiable and/or multiobjective optimisation, and wireless networks. His research interests are mathematical programming, non-smooth and non-convex optimisation, multiobjecitve problems, DTN network, and game theory.

This paper is a revised and expanded version of a paper entitled 'Analysis of the security between smart vehicles and parcels in smart cities' presented at The International Conference on Networking, Information Systems & Security (NISS 2018), FST-Tangier, Morocco, 27–28 April 2018.

1 Introduction

Intelligent transportation system (ITS) is becoming a mature technology: progress in standardisation and pre-deployment projects are paving the way for smart mobility. ITS offers innovative means of wireless communication between ITS stations and ITS road systems. They promote the development of ITS applications to improve road safety, traffic management, mobility and other services (Abdul Khaliq et al., 2017; Chunli, 2012). The ITS system must ensure the security of communications, especially in heterogeneous network environments. Applications that are critical in terms of security require authentication to prevent attackers from being able to send falsified or forged information, yet the confidentiality of vehicles and drivers must be maintained. In order to strengthen inter-vehicle cooperation, ITS exchanges relevant information on their speed, position, direction, etc., as well as emergency messages. Emergency messages and beacon messages will be used by ITS to understand their environment. These critical messages are security-sensitive, and the system must be robust to faulty devices or malicious users who may send erroneous or falsified information. To this end, it is essential to have a faulty behaviour detection mechanism that can monitor the system and exclude misplaced nodes.

In addition, the goal of 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 (Abdul Khaliq et al., 2017; Chunli, 2012).

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. Harmonisation and standardisation of collected and processed data, as well as the information delivered, form part of this overall ITS standardisation 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 modelled 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 communication between the smart vehicles and parcels in smart city (Wei and Wei, 2015; Pan et al., 2014; Alaoui et al., 2017). So, the main contributions of this paper can be summarised as follows:

The key contributions of this work are:

- to analyse 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 characterise the Nash equilibrium (NE) of each strategy.

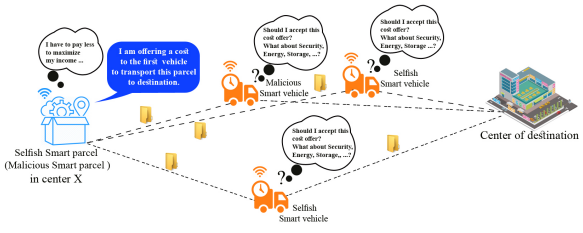
The rest of the paper is organised as follow: in Section 2 we describe our problematic. Then, we present an overview about ITS and IoT in Section 3 and 4, respectively. Section 5 provides analysis of interactions between the selfish smart vehicles/parcels and the malicious smart vehicles/parcels with special focus on game theory approach in smart cities. In Section 6, we analyse the game equilibria for selfish smart

vehicles/parcels and malicious smart vehicles/parcels. In Section 7, we will present the obtained results to assess the performance of the used our model. Finally, Section 8 is devoted to the conclusion.

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-centres 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 (see Figure 1).

Figure 1 Diagram explaining our problematic (see online version for colours)



3 Intelligent transport systems

ITS refers to intelligent transport systems (Zhou et al., 2012; Chunli, 2012). These are systems that process, analyse and communicate information about transportation systems. They are said to be intelligent because they are based on intelligence-related functions such as information processing, communication, memory and adaptation to imposed conditions. The purpose of ITS is to address societal issues that are targeted at the use of transportation. They are therefore anchored in a context of systems improvement for users as well as drivers and managers. Thus, ITS are present mainly in the management of traffic congestion and in the development of new information technologies embedded in vehicles. With regard to this last point one can find the domains of the simulation, telecommunication networks and real-time control. ITS therefore make it possible to improve the operation of the transportation system by various means. It is about saving time, minimising costs – mainly on the energy to use – productivity growth but also saving lives. ITS are present all over the world and are constantly being improved. In the transport industry or as consumers we sometimes use ITS without even knowing it (GPS, ADAS ...) (Zhou et al., 2012; Chunli, 2012).

The introduction of these new transport systems is encouraged, among other things, to reduce the risk of human errors and thus improve the safety of all. These systems are highly valued in our society, so it is normal to find them in the field of transport. For example, speed regulators or collision sensors are often present in new car models.

Systems that improve vehicle safety and vehicle-infrastructure co-ops are still evolving today. The goal is to implant them in new generations of vehicles. Another objective of ITS is the reduction of pollution caused by vehicles. This comes from better control of releases and the introduction of engines that consume less fuel (Zhou et al., 2012; Chunli, 2012).

4 Internet of things

4.1 Definition

Internet of things (IoT) (Lin et al., 2017; Aggarwal et al., 2013; Miorandi et al., 2012; Atzori et al., 2010) is able to improve to collect, analyse and retrieve data. These transformed into knowledge. It provides a real distribution of global resources to poor countries and helps to understand the planet. With this technology, we can adopt a more proactive behaviour instead of reacting to events. IoT represents the exchange of information and data from devices in the real world to the internet. In other words, this new concept refers to the interconnection in network of objects of daily life equipped with an omnipresent intelligence.

The Cluster of European Internet of Things Research Projects (CERP-IoT) defines the IoT as: "A dynamic infrastructure of a global network. This global network has autoconfiguration capabilities based on standards and interoperable communication protocols. In this network, physical and virtual objects have identities, physical attributes, virtual personalities and intelligent interfaces, and they integrated into the network in a transparent way".

The IoT concept focuses on easy use and secure manipulation to avoid potential threats and risks, while masking the underlying technological complexity. IoT aims to increase the ubiquity of the internet for the integration of each object for interaction via integrated systems (Lin et al., 2017). The IoT must design for easy use and secure manipulation to avoid potential threats and risks, while masking the underlying technological complexity.

4.2 Ecosystem of internet of things

The IoT ecosystem based on four steps (Aggarwal et al., 2013):

- *Collect and operate:* ultralight operating system (OS) designed for IoT, for example the fork of Android Brillo. These OS facilitate interactions between connected objects and smartphones. It intended to work on powerful or modest peripherals, with capability to connect a large number of possible objects.
- *Communicate:* a large number of communication techniques created, for objective: sending and receiving information, basing on two components that are the gateway and the router to the internet as satellites... The transferred data can be located and stored in distributed databases using cloud-computing technologies. The expected objective of this operation is the transmission of already collected data with minimal energy cost. Among those, Zigbee, Thread (Samsung, Google and ARM), SigFox...

- *Run:* this step will realised using platforms dedicated to the IoT. These platforms make it possible to:

  1 collect data

  2 transform and store data collected

  3 process and analyse this data

  4 provision and remotely monitor connected objects.

- *Visualise:* in the last step, a user interface must be created. This interface allows us to visualise the data as well as the interaction with the connected objects used. The smartphones, tablets and other mobile devices privileged to gain access to information regardless of location. Several developed mobile applications make it possible to control the smart objects used easily or to visualise the data collected.

5 Game formulation

In this work, to formally analyse 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 (Pan et al., 2014; Wei and Wei, 2015). We present a security non-cooperative game model that was inspired by the works in Alaoui et al. (2017).

In our model, the non-cooperative game model can be described as having three components:

Players: The set of the legitimate smart vehicles/parcels in 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, $\left\{P_{nj}^{D}\right\}_{j=1}^{m}$ and $\left\{P_{mj}^{C}\right\}_{j=1}^{m}$ 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 centres 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 shown as follows:

$$S = \{C, D\} \tag{1}$$

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 s. 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_{mj}^{C} is shown as follows

$$g_{mi}(x(s)) = q_{mi}(x(t)) \tag{2}$$

where q_{mi} is a positive parameter.

$f_{mi}(t)$ denotes the number of smart parcels that has been scheduled to transport and have successfully arrived at their centres of destination at time t by the selfish smart vehicle P_{mj}^{C}. For a collaborate smart vehicle/parcel P_{mj}^{C}, if a smart parcel originated from a selfish smart vehicle can be successfully delivered to its centre of destination, then the smart vehicle can get gain g_{mi}. For simplicity, $r_{mi}(f_{mi}(t))$ represents the smart parcels that have been scheduled to transport and have successfully arrived at their centres of destination, which is shown as follows:

$$r_{mi}(f_{mi}(t)) = f_{mi}(t)g_{mi} \tag{3}$$

where g_{mi} is a positive parameter.

$h_{nj}(i,t)$ denotes that a smart vehicle P_{nj}^{D} drops or injects the number of smart parcels, which are transported by the smart vehicle P_{mi}^{C} 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 $w_{nj}(h_{nj}(i,t))$. For simplicity, the gains $w_{nj}(h_{nj}(i,t))$ of the malicious smart vehicle P_{nj}^{D} is shown as follows:

$$w_{nj}(h_{nj}(i,t)) = (1 - x(s))h_{nj}(i,t)c \tag{4}$$

where c is a positive constant.

In the work, $u_i(s)$ 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.

$$u_i(s) = \frac{\text{resource consume at time } s}{\text{the total of smart vehicle/parcel } i} \tag{5}$$

Assume that the cost paid by the selfish smart vehicle/parcel P_{mi}^{C} is shown as follows:

$$y_{mi}(u_{mi}(s)) = \frac{c_{mi}}{2}u_{mi}(s)^2 \tag{6}$$

And the cost paid by the malicious smart vehicle/parcel P_{nj}^{D} is shown as follows:

$$y_{nj}(u_{nj}(s)) = \frac{c_{nj}}{2}u_{nj}(s)^2 \tag{7}$$

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

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

$$U_{mi} = \int_{t_0}^{T} \left[q_{mi}x(t) + f_{mi}(t)g_{mi} - \frac{c_{mi}}{2}u_{mi}(s)^2 \right] e^{(-r(s-t_0))}\mathrm{d}s + e^{(-r(T-t_0))}S_{mi}x(T) \tag{8}$$

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}^{C} 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 centre. Similarly, for a malicious smart vehicle/parcel P_{nj}^{D}, we can model the malicious smart vehicles/parcels' utility function as follows

$$U_{nj} = \int_{t_0}^{T} [q_{nj}(1 - x(s)) + (1 - x(s))h_{nj}(i,s)c - \frac{c_{nj}}{2}u_{nj}(s)^2 \Big] e^{(-r(s-t_0))}\mathrm{d}s + e^{(-r(T-t_0))}S_{nj}[1 - x(T)] \tag{9}$$

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

$$\begin{aligned} &\frac{dx(s)}{ds} = \sum_{i=1}^{m} u_{mi}(s)[1 - x(s)]^{1/2} - \sum_{j=1}^{n} u_{nj}(s)x(s)^{1/2} \\ &x(0) = x_0 \end{aligned} \tag{10}$$

6 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 turn to study the node's behaviour and characterise 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. $u_i(s)$

6.1 Nash equilibrium solution for the selfish smart vehicles/parcels

Let $u_{mi}^{(t_0)*}(t,x) = [u_{m1}^{(t_0)*}(t,x),\ u_{m2}^{(t_0)*}(t,x),\ \ldots,\ u_{mm}^{(t_0)*}(t,x),\ u_{n1}^{(t_0)*}(t,x),\ u_{n2}^{(t_0)*}(t,x),\ \ldots,\ u_{nn}^{(t_0)*}(t,x)]$, for $t \in [t_0, T]$ denotes a set of strategies that provides a Nash equilibrium solution to the non-cooperative game.

$\Gamma(x_0, T - t_0)$ and $W^{(t_0)t}(t,x) : [t_0, T] \times \mathbb{R}^n \to \mathbb{R}$ denotes the value function of the selfish smart vehicles/parcels P_{mi}^{C}.

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

$$\begin{aligned} -V_t^{(t_0)mi}(t,x) = \max_{U_{mi}} \{ & [q_{mi}x(t) + f_{mi}(t)g_{mi} - \frac{c_{mi}}{2}u_{mi}(t)^2]e^{-r(t-t0)} \\ & + V_x^{mi}(t,x)[u_{mi}(t)[1 - x(t)]^{1/2} \\ & + \sum_{k \neq i=1}^{m} u_{mk}^{*}(t,x)[1 - x(t)]^{1/2} \\ & - \sum_{j=1}^{n} u_{nj}^{*}(t,x)x(t)^{1/2}] \} \\ V^{mi}(T,x) = e^{-r(T-t_0)}S_{mi}x, & \end{aligned} \tag{11}$$

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

$$u_{mi}^{(t_0)*}(t,x) = \frac{V_x^{mi}(t,x)}{c_{mi}}(1-x)^{1/2}e^{r(t-t_0)} \quad \text{for } i \in \{1, 2, \ldots, m\}. \tag{12}$$

6.2 Nash equilibrium solution for the malicious smart vehicles/parcels

For malicious smart vehicles/parcels $P_{nj}^{D},\ j \in \{1, 2, \ldots, n\}$ a feedback Nash equilibrium solution to the equations (9) and (10) has to satisfy the following conditions

$$\begin{aligned} -V_t^{(t_0)nj}(t,x) = \max_{U_{nj}} \{ & [q_{nj}(1 - x(t)) + (1 - x(t))h_{nj}(i,t)c \\ & - \frac{c_{nj}}{2}u_{nj}(t)^2]e^{-r(t-t0)} + V_x^{nj}(t,x)[-u_{nj}(t)[x(t)]^{1/2} \\ & + \sum_{i=1}^{m} u_{mi}^{*}(t,x)[1 - x(t)]^{1/2} \\ & - \sum_{l \neq j=1}^{n} u_{nl}^{*}(t,x)x(t)^{1/2}] \} \end{aligned} \tag{13}$$

$$V^{nj}(T,x) = e^{-r(T-t_0)}S_{nj}(1-x), \tag{14}$$

Similarly, the Nash equilibrium solution for the malicious smart vehicles/parcels by performing the indicated maximisation in equation (14) yields,

$$u_{nj}^{(t_0)*}(t,x) = \frac{-V_x^{nj}(t,x)}{c_{nj}}x^{1/2}e^{r(t-t_0)} \quad \text{for } j \in \{1, 2, \ldots, n\}. \tag{15}$$

Upon substituting $u_{mi}^{(t_0)*}(t,x)$ and $u_{nj}^{(t_0)*}(t,x)$ into (11) and (14), respectively, and solving (11) and (14), we obtain the value functions

$$V^{mi}(t,x) = e^{-r(t-t_0)}[A_{mi}(t)x + B_{mi}(t),], \text{for } i \in \{1,2\ldots,m\}, \tag{16}$$

$$V^{nj}(t,x) = e^{-r(t-t_0)}[A_{nj}(t)(1-x) + B_{nj}(t),], \quad \text{for } j \in \{1,2,\ldots,n\}. \tag{17}$$

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

$$\frac{A_{mi}(t)}{dt} = rA_{mi}(t) - q_{mi} + \frac{A_{mi}^2(t)}{2c_{mi}} + \sum_{k\neq i=1}^{m} \frac{A_{mi}(t)A_{mk}(t)}{c_{mk}} + \sum_{j=1}^{n} \frac{A_{mi}(t)A_{nj}(t)}{c_{nj}} \tag{18}$$

$$A_{mi}(T) = S_{mi} \tag{19}$$

$$\frac{B_{mi}(t)}{dt} = rB_{mi}(t) - f_{mi}g_{mi} - \frac{A_{mi}^2(t)}{2c_{mi}} - \sum_{k\neq i=1}^{m} \frac{A_{mi}(t)A_{mk}(t)}{c_{mk}} \tag{20}$$

$$B_{mi}(T) = 0 \tag{21}$$

$$\frac{A_{nj}(t)}{dt} = rA_{nj}(t) - q_{nj} - h_{nj}c + \frac{A_{nj}^2(t)}{2c_{nj}} + \sum_{l\neq j=1}^{n} \frac{A_{nj}(t)A_{nl}(t)}{c_{nl}} + \sum_{i=1}^{m} \frac{A_{mi}(t)A_{nj}(t)}{c_{mi}} \tag{22}$$

$$A_{nj}(T) = S_{nj} \tag{23}$$

$$\frac{B_{nj}(t)}{dt} = rB_{nj}(t) - q_{nj} - h_{nj}c + \sum_{i=1}^{m} \frac{A_{mi}(t)A_{nj}(t)}{c_{mi}} \tag{24}$$

For the symmetric case, (18) becomes

$$B_{nj}(T) = 0. \tag{25}$$

$$\frac{A_{mi}(t)}{dt} = rA_{mi}(t) + (m-1/2)\frac{A_{mi}^2(t)}{c_{mi}} + n\frac{A_{mi}(t)A_{nj}(t)}{c_{nj}} - q_{mi} - h_{nj}c. \tag{26}$$

Similarly, we have that

$$\frac{A_{nj}(t)}{dt} = rA_{nj}(t) - q_{nj} - h_{nj}c + \left(n - \frac{1}{2}\right)\frac{A_{nj}^2(t)}{c_{nj}} + m\frac{A_{mi}(t)A_{nj}(t)}{c_{mi}}. \tag{27}$$

Upon substituting the relevant partial derivatives of $V^{mi}(t,x)$ and $V^{nj}(t,x)$ from (16) and (17) into (12) and (15) yields the feedback Nash equilibrium strategies

$$u_{mi}^{(t_0)*}(t,x) = \frac{A_{mi}(t)}{c_{mi}}(1-x)^{1/2} \quad \text{for the selfish smart vehicle/parcel } P_{mi}^{C},\ i \in \{1,2,\ldots,m\} \tag{28}$$

and

$$u_{nj}^{(t_0)*}(t,x) = \frac{A_{nj}(t)}{c_{nj}} x^{1/2} \quad \text{for the selfish smart vehicle/parcel } P_{nj}^{D},\ j \in \{1,2,\ldots,n\}. \tag{29}$$

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

$$\frac{dx(s)}{ds} = -\left(\sum_{i=1}^{m} \frac{A_{mi}(t)}{c_{mi}} + \sum_{j=1}^{n} \frac{A_{nj}(t)}{c_{nj}}\right) x(s) + \sum_{i=1}^{m} \frac{A_{mi}(t)}{c_{mi}} \tag{30}$$

$$x(0) = x_0 \tag{31}$$

$$x^*(t) = \bar{\omega}(t_0,t)\left(\int_{t_0}^{t} \left[\frac{A_{mi}(t)}{c_{mi}}\right] \bar{\omega}^{-1}(t_0,t)ds + x_0\right), \quad \text{for } t \in [t_0,T], \tag{32}$$

where

$$\bar{\omega}(t_0,t) = e^{-\int_{t_0}^{t} H(\tau)d\tau} \tag{33}$$

and

$$H(s) = -\left(\sum_{i=1}^{m} \frac{A_{mi}(t)}{c_{mi}} + \sum_{j=1}^{n} \frac{A_{nj}(t)}{c_{nj}}\right) \tag{34}$$

The Nash equilibrium strategies, $u_{mi}^{(t_0)*}(t,x)$ and $u_{nj}^{(t_0)*}(t,x)$, 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.

7 Results and discussions

In order to verify the performance of the non-cooperative model that we proposed, here is a numerical example. The following example consists of two groups of smart vehicles/parcels, selfish and malicious ones. There are up to 1,000 selfish smart vehicles/parcels and 200 malicious smart vehicles/parcels, when we look at the IoT. The time of start is set to 0, i.e., $t_0 = 0$. Tables 1 and 2 show the parameter settings for the selfish and malicious smart vehicles/parcels in this example, respectively.

In both Tables 1 and 2, values that are received at time t are discounted by a factor of r, with $r > 0$ being the discount rate. Also, $S_{mi}(x(T))$ defines the marginal utility of all selfish smart vehicles/parcels, while $S_{nj}(1 - x(T))$ defines the marginal utility of malicious smart vehicles/parcels, at time T. Our time interval is defined by $T = [2,4]$.

Table 1 Parameters of simulation for the selfish for smart vehicles/parcels

Parameter	*Value*
q_{mi}	8.7
f_{mi}	12
c_{mi}	1.8
g_{mi}	8
$S_{mi}(x(T))$	2.5
r	$r > 0$
c	7
T	[2, 4] hour

Table 2 Parameters of simulation for the malicious smart vehicles/parcels

Parameter	*Value*
q_{nj}	6.5
$h_{nj}(i,t)$	3
c_{nj}	2.5
$S_{nj}(1-x(T))$	1.7
r	$r > 0$
c	7
T	[2, 4] hour

Figure 2 Variations in the values of $A_{mi}(t)$ and $A_{nj}(t)$ in time t (see online version for colours)

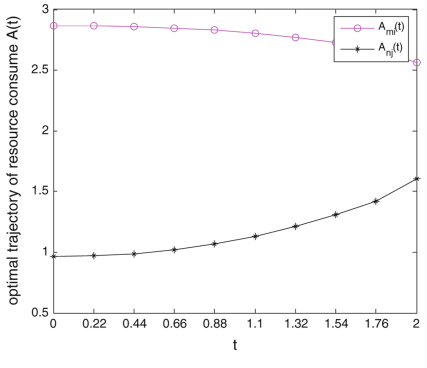


Figure 2 illustrates variations in the values of $A_{mi}(t)$ and $A_{nj}(t)$ in time t. We can easily see that there is a decrease in the values of $A_{mi}(t)$ in the interval $t \in [0, 2[$ hour, while the values of $A_{nj}(t)$ increase over time. In (28) and (29), the feedback that is expected from the Nash equilibrium strategies, $u_{mi}^{(t_0)*}(t,x)$ and $u_{nj}^{(t_0)*}(t,x)$ are a function of A_{mi} and A_{nj} respectively. Those will significantly influence how much node's optimal strategies vary. Therefore, the optimal amount of network resources that

should be invested in information security, or used to attack each smart vehicle/parcel of the network in the IoT, will have a variation of A_{mi} and A_{nj}.

Figure 3 illustrates, with game time $t \in [0, 2]$ hour, the relationship between optimal trajectories u_{nj} and u_{mi}. Also, this figure shows the optimal quantity of network resources invested in information security, while using the feedback of Nash equilibrium strategies $u_{mi}^{(t_0)*}(t, x)$ and $u_{nj}^{(t_0)*}(t, x)$. The optimal quantity varies with each security mechanisms when $t \in [0, 2]$ hour. We observe an decrease over time $t \in [0, 2]$ hour of selfish smart vehicles/parcels' values of u_{mi}, while in the same time frame malicious smart vehicles/parcels' values of u_{nj} increases, which will lead to more overhead. Practically speaking, selfish smart vehicles/parcels aim to conserve their limited resources. Instead, malicious smart vehicles/parcels will try to damage the network without putting a priority on saving limited resources.

Figure 3 Relationship between optimal trajectories u_{nj} and u_{mi} with game time $t \in [0, 2]$ hour (see online version for colours)

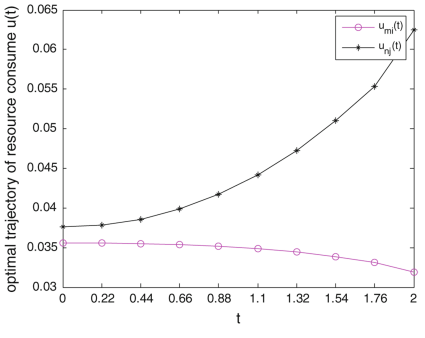
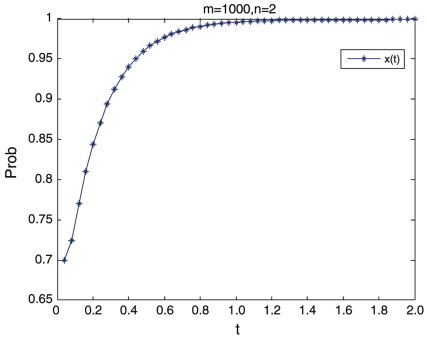


Figure 4 Relation between the probability $x(t)$ that the selfish nodes discover the malicious nodes game time $t \in [0, 2]$ hour with 1,000 selfish nodes, two malicious nodes and $T = 2$ hour (see online version for colours)



We begin with the case where the total number of selfish nodes and the total number of malicious nodes are equal to 1,000 and 2, respectivly, in the IoT. Figures 4 and 5 show that, under the optimal strategies $u_{nj}(t)$ and $u_{mi}(t)$, the probability $x(t)$ that the selfish nodes discover the malicious nodes increases from 70% to 100% in 1.2 hours.

We consider now the case where total number of selfish nodes and the total number of malicious nodes are equal to 1,000 and 50, respectivly, in the IoT. Also, Figures 6 and 7 show that, under the optimal strategies $u_{nj}(t)$ and $u_{mi}(t)$, the probability $x(t)$ that the selfish nodes discover the malicious nodes increases from 70% to 97.5% in 1.2 hours.

Figure 5 Relation between the probability $x(t)$ that the selfish nodes discover the malicious nodes game time $t \in [0, 4]$ hour with 1,000 selfish nodes, two malicious nodes, and $T = 4$ hour (see online version for colours)

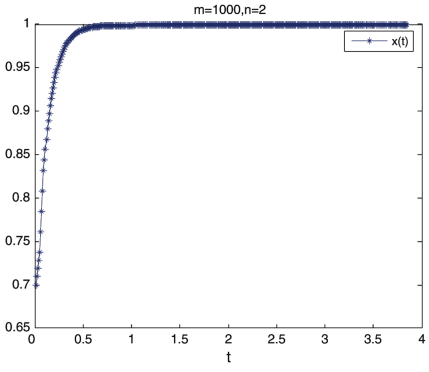


Figure 6 Relation between the probability x(t) that the selfish nodes discover the malicious nodes game time $t \in [0, 2]$ hour with 1,000 selfish nodes, 50 malicious nodes $T = 2$ hour (see online version for colours)

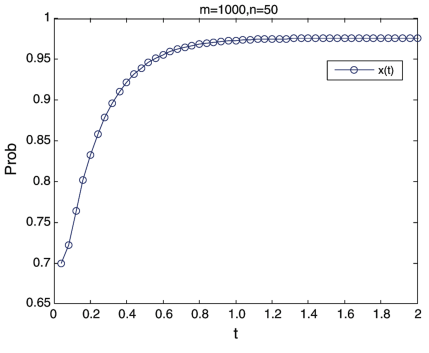
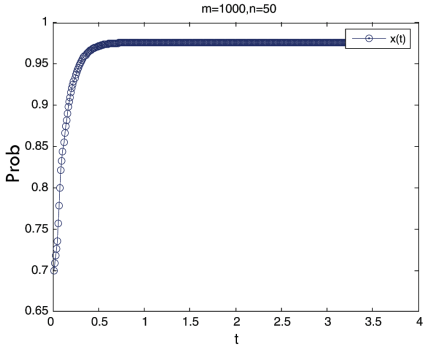


Figure 7 Relation between the probability x(t) that the selfish nodes discover the malicious nodes game time $t \in [0, 4]$ hour with 1,000 selfish nodes, 50 malicious nodes and $T = 4$ hour (see online version for colours)



These results (in Figures 4, 5, 6 and 7) show that our game model has a good performance in terms of the number of the malicious nodes and the stability of the probability that the selfish nodes discover the malicious nodes, under the optimal strategies of the selfish.

8 Conclusions

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

References

Abdul Khaliq, K., Qayyum, A. and Pannek, J. (2017) 'Novel routing framework for VANET considering challenges for safety application in city logistics', *Vehicular Ad-Hoc Networks for Smart Cities*, Vol. 548, pp.53–67.

Aggarwal, C.C., Ashish, N. and Sheth, A. (2013) 'The internet of things: a survey from the data-centric perspective', *Managing and Mining Sensor Data*, pp.383–428, Springer.

Alaoui, E.A.A., Nassiri, K. and El Moudden, M. (2017) 'Framework for analysing of inter-cluster communication in the DRHT by using game theory', *The Mediterranean Symposium on Smart City Applications (SCAMS 2017)*, 25–27 October, Tangier, Morocco, ACM.

Atzori, L., Iera, A. and Morabito, G. (2010) 'The internet of things: a survey', *Computer Networks*, Vol. 54, No. 15, pp.2787–2805.

Chunli, L. (2012) 'Intelligent transportation based on the internet of things', *IEEE 2nd International Conference on Consumer Electronics, Communications and Networks*, IEEE.

Dimitrakopoulos, G., Demestichas, P. and Koutra, V. (2012) 'Intelligent management functionality for improving transportation efficiency by means of the car pooling concept', *IEEE Trans. Intell. Transp. Syst.*, pp.424–436.

El-Azouzi, R., Pellegrini, F. and Kamble, V. (2010) 'Evolutionary forwarding games in delay tolerant networks', *Proceedings of the 8th International Symposium o Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, pp.81–89, IEEE.

Elhenawy, M., Elbery, A. and Hassan, A. (2015) 'An intersection game-theory-based traffic control algorithm in a connected vehicle environment', *IEEE 18th International Conference on Intelligent Transportation Systems*, IEEE.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. and Zhao, W. (2017) 'A survey on internet of things: architecture, enabling technologies, security and privacy, and applications', *IEEE Internet of Things Journal*, Vol. 4, No. 5, pp.1125–1142.

Liu, Q., Pang, X., Wang, Y. and Li, L. (2012) 'An improved path management policy for the ferry in opportunistic networks', *Journal of Networks*, Vol. 7, No. 10, pp.1568–1575.

Miorandi, D., Sicari, S., de Pellegrini, F. and Chlamtac, I. (2012) 'Internet of things: vision, applications and research challenges', *Ad Hoc Networks*, Vol. 10, No. 7, pp.1497–1516, Springer.

Pan, F., Xi, B. and Wang, L. (2014) 'Environmental regulation strategy analysis of local government based on evolutionary game theory', *2014 International Conference on Management Science and Engineering (ICMSE)*.

Roumboutsos, A. and Kapros, S. (2008) 'A game theory approach to urban public transport integration policy', *Transport Policy*, Vol. 19, pp.209–215, Elsevier.

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

Zhou, H., Liu, B. and Wang, D. (2012) 'Design and research of urban intelligent transportation system based on the internet of things', *Internet of Things*, pp.572–580, Springer, Berlin, Heidelberg.