A Game Theoretic Approach for Privacy Preserving Model in IoT-Based Transportation

Arbia Riahi Sfar, Yacine Challal, Pascal Moyal, Enrico Natalizio

A game theoretic approach for privacy preserving model in IoT-based transportation

Arbia Riahi Sfar*‡, Yacine Challal§, Pascal Moyal¶‡, Enrico Natalizio†
* Military Academy of Tunisia, VRIT Lab, Nabeul, Tunisia. e-mail: arbia.sfar@hds.utc.fr
§ Ecole Nationale Supérieure d'Informatique, LMCS, Algeria. e-mail: y_challal@esi.dz
‡ Sorbonne Universités, UTC, CNRS. ¶ Université de Lorraine, IECL. e-mail: pascal.moyal@utc.fr
† Université de Lorraine, LORIA, CNRS UMR 7503, Inria. e-mail: enrico.natalizio@loria.fr

***Abstract*—Internet of Things (IoT) applications using sensors and actuators raise new privacy related threats such as drivers and vehicles tracking and profiling. These threats can be addressed by developing adaptive and context-aware privacy protection solutions to face the environmental constraints (memory, energy, communication channel, etc.), which cause a number of limitations of applying cryptographic schemes. This paper proposes a privacy preserving solution in ITS context relying on a game theory model between two actors (data holder and data requester) using an incentive motivation against a privacy concession, or leading an active attack. We describe the game elements (actors, roles, states, strategies, and transitions), and find an equilibrium point reaching a compromise between privacy concessions and incentive motivation. Finally, we present numerical results to analyze and evaluate the game theory-based theoretical formulation.**

***Index Terms*—Internet of Things, intelligent transportation, privacy, game theory, Markov chains.**

I. Introduction

The evolution of IoT invokes massive possibilities for exchanging private data enabling new business models across heterogeneous networks. Intelligent Transportation Systems (ITS) noticed a fast development in communication technologies as one of the key founders of IoT, and provides numerous applications to solve problems related to modern transportation environment. Authors in [1] surveyed the Internet of Vehicles (IoV) in big data era, and investigated the application of IoV big data in autonomous vehicles, and discussed the emerging issues. One of the most important applications is transport logistics, which ensure various capabilities as real time cargo and goods tracking/location, automate scheduling/delivery, and vehicles capacity management.

Due to the dynamic nature of the entities, their interactions, and the topology of the network, new privacy and security issues arise. Based on information such as identities, pseudonyms, locations, and profiles; an enemy can initiate active or passive attacks to thieve social data or to damage communications. For instance, the rising security and privacy issues of Mobile Social Networks (MSN) are strongly related to the application design and the user's needs. Commonly, during MSN applications conception, security and privacy aspects such as the trust relations, private information leakage, and malicious behavior, need to be considered [2].

As IoT devices are known for their limited memory space and computational capabilities, conventional solutions, as encryption methods, are inadequate to solve many privacy concerns. One promising solution is the use of game theory to model interactions between actors and assist them during decision making to balance valuable vehicular social information with personal and private information. Many papers have considered both game-based or payoff-based dynamical system, such as [3], where authors dealt with evolutionary stability in games of communication. In [4], author considered game theory from the perspective of quantum algorithms, and in [5] statistical mechanics of voting are debated. Recently, a distributed, dynamical system view of finite, static games was proposed in [6].

In this paper, we propose a game theory-based privacy preservation model between data holder (driver, intelligent devices, etc.) and data requester (employer, supplier, etc.), to find the optimal protection strategy for a data holder to preserve private data over a series of interactions with a data requester. We define a set of states for each player and we use a Markovian chain to model transitions. An utility function is proposed to evaluate the compromise between privacy concession and incentive motivation, and make the adequate decision of disclosing private data or not.

The remaining of this paper is organized as follows. Section II depicts the most important research activities related to the use of game theory to solve privacy concerns in IoT-based applications. Section III discusses the privacy issues in ITS and lists the most important attacks of automated vehicles. Section IV presents the overall architecture of an ITS using game theory in privacy preservation. Section V explains game strategies, actors, equilibrium and utility function. Section VI presents numerical results; and the last section concludes the paper and proposes possible future directions.

II. Related work

In literature, many approaches have been proposed to protect privacy, and a whole bunch of privacy negotiation tools and research can be explored. Applications examples include Windows CardSpace[1], the Microsoft's client software for the Identity Metasystem, Idemix[2] (Identity Mixer), and P3P[3] (Platform for Privacy Preferences Project). Besides, a great deal of effort was made in data minimization, anonymity and unlinkability [7]–[9]. Some of the most prominent research proposals debating privacy in IoT environments are summarized in table I where we use three parameters: input measures (adversary's estimate, adversary's resources, true outcome, prior knowledge, parameters), output measures (uncertainty, information gain or loss, similarity/diversity, indistinguishability, adversary's success probability, error, time, accuracy/precision) [10], and privacy properties (anonymity, pseudonymity, unlinkability, and unobservability)[4], to compare our work to anonymization (k-Anonymity, l-Diversity, t-Closeness, PPDP/PPDM), cryptography, blocking approaches, and differential privacy.

Due to its mathematical rigor and its numerous solutions, many researchers choose to use game theory in formulating interactions between actors in security scenarios. In [11], a Stackelberg Bayesian game between the user and the company was proposed to make a rational decision of the service provider in conjunction with rational decision-making of the users who wish to protect their location privacy. However, authors did not provide any information theory-based metrics, and did not consider active attacks scenarios. In [12], authors focused on location privacy, where a defender uses the privacy protecting techniques against the attack strategies implemented by an adversary. They consider both passive and active attack scenarios, and proposed complete information and incomplete information games. Nevertheless, their work consider only location privacy information and did not provide any privacy quantification method. To enhanced information usage in online information service, authors in [13] integrated privacy protection methodology into the process of shared data generation and consumption, under a differential privacy framework. In [14], authors proposed a novel unified approach, parallel driving, a cloud-based cyberphysical social systems framework aiming at synergizing connected automated driving. Although their considerable contribution in automotive technology, they did not debated security aspects. In [15], authors proposed a privacy-provable and deployable framework for Vehicular Location-Based Services (VLBS) based on computational Private Information Retrieval (cPIR); and guaranteed much lower communication cost for VLBS.

Solutions	Input Measures	Output Measures	Priv. Prop.
Anonym.	- Adv. estimate - Parameters - True Outcome	- Uncertainty - Similarity /diversity - Adv. success prob.	- Anonymity - Pseudonymity - Unlinkability
Crypto.	- Adv. Resources - True Outcome - Parameters	Indistinguishability	Unobservability
Blocking App.	- Adv. estimate - Parameters - True outcome	- Adv. success prob. - Time	Unobservability
Differential privacy	- True Outcome - Adv. estimate - Parameters	- Inf. gain or loss - Indistinguishability	- Anonymity - Unlinkability
Proposed model	- Adv. Estimate - Adv. Resources - True Outcome - Prior knowl. - Parameters	- Inf. gain or loss - Adv. success prob. - Uncertainty - Time	Unobservability

TABLE I
Summary of privacy preservation models.

As stochastic games can be used to model the interactions between malicious attackers and defenders, we adopt their principle to deal with privacy concerns in ITS scenarios. They capture interactions between game players and system's dynamics, to compute probabilities of expected adversary behavior, build a transition matrix, and evaluate the interconnected system security.

III. Recent attacks and privacy issues of connected vehicles

ITS core technologies include reliable and real-time platforms managing mixed vehicle services, efficient navigation, improved decision-making algorithms, communication and network technologies, and open service platform. They enable interactions among sensors, vehicles, drivers and supervisors, and integrate features of both vehicular networks and social networks, which raise considerable privacy issues. In figure 1, an abstract model of data exchange vectors in the vehicular communication domain is shown, and attack surfaces are highlighted. For example, location privacy issues may be caused by unencrypted messages (identifier, location, speed, etc.) exchanged over the network, which may be linked to driver's identity and lead to identity theft, tracking and users linkage. Consequently, the system can be abused by third parties (employers, insurance companies, criminals) to track individuals, and re-identify anonymous users in a social network graph [16].

From security point of view, these systems are exposed to many risks as attacking autonomous vehicle sensors including wheel encoder, on-board unit, e-maps, ultrasonic sensors, radar, camera, GPS, wireless cards, etc. Many security attacks may occur such as jamming, replay, relay, spoofing, tracking, and blinding. To highlight the seriousness of privacy concerns, we summarize the most important attacks during the last few years in table II.

[1] msdn.microsoft.com
[2] idemix.wordpress.com/
[3] www.w3.org/P3P/
[4] www.commoncriteriaportal.org
[5] www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Date	Attack	Description
Jul. 2015	Miller and Valasek Remote Hack	Attackers demonstrated that a 2014's Jeep Cherokee could be remotely exploited without the need for any physical access to gain remote access and execute code[5].
Jul. 2015	Jeep Cherokee controlled through its "Uconnect" infotainment system	Hackers managed to send commands to the dashboard functions, transmission, brakes, and steering remotely. The company recalled 1.4 million vehicles to fix the security flaw[6].
Apr. 2016	BMW, Audi and Toyota cars can be unlocked and started with hacked radios	The hack uses a simple radio amplifier, and involves 24 different car models from 19 manufacturers, with keyless-entry systems, which send a radio signal from the car to the key when the owner is a short distance away that opens the car door[7].
Nov. 2016	Hack attack of the metro transport systems in San Francisco	Hackers forced the agency to shut down its light-rail ticketing machines and allowing passengers to ride for free. Ticket machines display : "You hacked. ALL data encrypted "[8].
Aug. 2017	Hack attack of highway message boards in California.	Hackers managed the electronic message board to bypass the password and post their Anti-Trump message[9].

TABLE II
RECENT ATTACKS OF CONNECTED CARS.

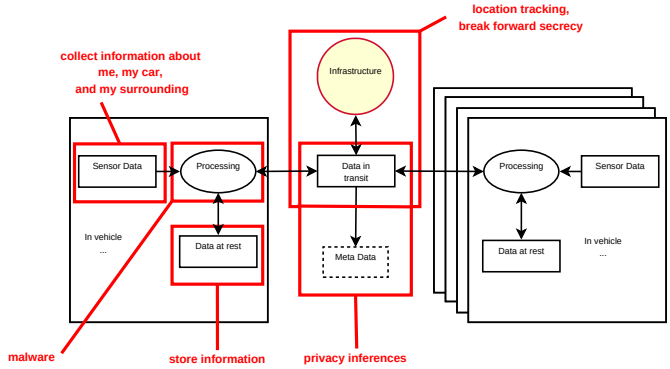


Fig. 1. Privacy violation in connected cars [17].

To avoid threats, countermeasures such as detect jamming attacks on cameras via spectral analysis, increase redundancy by adding cameras, etc. may be taken [17].

In [18], SANS institute proposed four main solutions to prevent car hacking. First, cryptography methods may be used to solve the lack of message confidentiality problems, but may be affected by the maximum data field size allowed by CAN protocol's. Second, the use of device authorization may prevent unauthorized computers or CAN controllers from broadcasting CAN messages, but requires additional processing time to CAN transmissions, additional expense for automakers, and additional weight on the vehicle. Third, defense in depth provides multiple layers security but needs to find a balance between the protection capability and cost, performance, and operations considerations. Fourth, security by design may be considered into vehicle systems from the ground up, but many security problems were caused by the lack of features due to the development of programs before cars were connected to Internet, and automobile industry which moves slowly and resists change. These challenges affect the whole IoT ecosystem, and may lead to devices failure, or even to serious exposure to danger. For example, many difficulties about managing cryptographic material may occur (key renewal, update, recovery, etc.). In some particular situations, cryptography implementation may be expensive, or unsuitable in environments with constrained energy consumption.

To develop more realistic models of interactions between untrusted entities, researchers accord significant interest in combining game theory techniques and cryptographic schemes [19]. Many game theoretic approaches were proposed recently to explore practical and defensible ways of safeguarding connected cars against many types of abuse, including static, cooperation, sequence, and traceability games [20]. This can be explained by the fact that both game theory and cryptography are concerned with interactions among entities with conflicting interests. In the cryptographic setting, a set of communicating entities aim to evaluate a function on their inputs, and receive some output of the computation. To face malicious behavior, cryptography guarantees properties such as secrecy, correctness and fairness. Game theory is more open-ended, by understanding natural behaviors and goals of entities, and conceiving a set of rules leading to decisions with desirable properties. It guarantees some payoff for the players according to their joint actions [21]. Thus, ideas from both disciplines may be combined to model interaction with conflicting interests.

IV. PROPOSED MODEL

We propose a solution for privacy preservation using game theory, which can be used to complete cryptographic mechanisms. To position our work, we use the Common Criteria Privacy Components[10] (anonymity, pseudonymity, unlinkability, unobservability). We aim to assure unobservability using data protection, to mitigate the attacks of location tracking and break forward secrecy (shown in figure 1). An illustrative example of IoT application in ITS field is shown in figure 2. By using a recently proposed systemic and cognitive approach for security in IoT [22]–[24], we can distinguish four main stakeholders: person (users, drivers, experts, etc.), technological ecosystem (software, robotics, networks, etc.), process (manufacturing, integration, etc.), and intelligent objects (sensors, RFID, monitoring equipment, payment devices, etc.). In this scenario, we assume that

[6] www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[7] www.telegraph.co.uk/technology/2016/03/23/hackers-can-unlock-and-start-dozens-of-high-end-cars-through-the/
[8] www.cnbc.com/2016/11/28/cybersecurity-experts-.html
[9] www.hackread.com/road-sign-in-modesto-hacked-with-anti-trump-message/
[10] www.commoncriteriaportal.org

private data are hold by sensors, intelligent vehicles and drivers. They are connected to employer/supervisor to optimize the movement of people and products, improve financial profit, public safety, and the environment, etc.

More precisely, we consider the fleet management domain where ITS service providers (insurance companies, criminals , advertisement) may attempt to access sensing data to improve their activities. They may carry an attack or encourage data holder through incentive motivation. We define a game involving two players that use their goals, believes and intentions to make real-time decisions to protects their interests. As we believe that road security can not be negotiated, our approach is not suitable for exchanges related to emergency situations. As nowadays vehicles are already complex systems with many computers and integrated sensors, and able to collect information and exchange them in real time with other vehicles [25], we adopt the on-vehicle computation (utility function, steady state, etc.) option.

A. Model description

In the scenario presented in figure 2, two types of players are involved: Data Holder (DH) and Data Requester (DR). DH may be a sensor or a driver, and may sell its sensing data if the DR offers a motivating buying price and a minimum privacy preference level is respected. DR may be a supervisor or a service provider, and may lead an attack to access sensing data or attempt to buy them from a particular driver or a set of sensors. In this work, we suppose the existence of an automated data acquisition process, a data detection and data categorization mechanism to determine driver's identification and activities, as well as to track commercial vehicles and determine driver's health and environmental data. To define an adequate pricing model for private data, many solutions are given in [26]. In practice, we can adopt utility maximization pricing schemes which describe the level of preference that a player receives from consuming goods or services. Regarding the attack model, we distinguish two cases: *passive attack* where the adversary's goal is to read private information without providing any effort to find potential victims, and *active attack* where the adversary is active by providing effort to encounter victims and to identify private data [12].

B. Actors and game players

Game players/actors and roles are summarized in table III where we propose two different scenarios. In the *incentive* scenario, DH owns the private data and DR is a curious player which proposes an incentive motivation value to access private data. In the *attack* scenario, DR is a malicious player which leads an attack to access private data. Income and expense of each player differ in both scenarios according to the player strategy. When

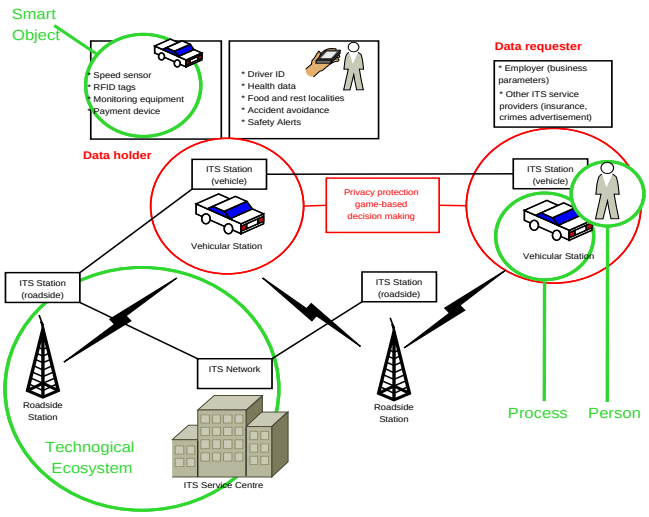


Fig. 2. Overall architecture of IoT-based ITS application.

the equilibrium is reached, players are either satisfied by the realized balance between data privacy and incentive motivation, or stop the game to minimize expenses.

V. Game theoretic formulation

A. Utility functions

The utility function of a player pl, U_{pl} expresses the preferences over outcomes. He/she prefers outcome a to outcome a' if $U_{pl}(a) > U_{pl}(a')$. It considers the privacy concession made by DH and the incentive motivation proposed by DR. During the game, DR aims to access private data, and is not directly concerned by privacy concession. Then, we believe that DH is the key player of the game, and the utility function reflects his/her ability to disclose or not private data against an interesting incentive motivation. To remain applicable in the attack scenario where no incentive are proposed, this function will be adapted with a null incentive value.

We consider two sub-functions: a loss function, denoted by L, which returns the privacy concession, and a gain function G, which represents the impact of the incentive motivation on the player. Mathematically, we chose to use sigmoid functions for L and G because they provide a good example of non-linear and quickly increasing functions of the probability of disclosure, and makes computation easier than arbitrary activation functions.

$$L(p_{priv}) = \frac{1}{1 + e^{-g_{priv} * (p_{priv} - h_{priv})}};$$

$$G(p_{inc}) = \frac{1}{1 + e^{-g_{inc} * (p_{inc} - h_{inc})}}$$

where g_{priv} and g_{inc} are the steepness of sigmoid functions, and h_{priv} and h_{inc} are their centers. In practice, g_{priv} depends on user preferences and realized privacy, and g_{inc} depends on motivation value proposed

	Player	System component	Role	Actions	Payoffs	Implications of equilibrium
Scenario 1: Incentive	DH	Sensors, drivers	Chooses to disclose data or reject request	Wait, Negotiate (sell), Disclose, Reject.	**Income**: incentives. **Expense**: privacy concession	DH and DR are satisfied with privacy concession and incentive motivation
	DR	Supervisor, provider, users	Chooses an incentive value paid for DH	Wait, Negotiate (buy), Stop (wait)	**Income**: access to private data **Expense** : incentives	
Scenario 2: Attack	DH	Sensors, drivers	Defends data privacy	Wait, A/D (defend), Disclose, Reject	**Income**: none **Expense**: privacy loss of sensitive data	DR succeeds to access private data or recognizes his/her failure
	DR	Attacker	Leads an attack to access private data	Wait, A/D (attack), Stop (wait)	**Income**: access to private data **Expense**: attack cost	

TABLE III
SCENARIOS, PLAYERS, ROLES AND ACTIONS OF THE GAME.

by DR, and an external constant reflecting the market conditions. p_{priv} is the probability of making privacy concession by DH, and p_{inc} is the probability of accepting the incentive motivation proposed by DR. Observe that these two probabilities are defined independently, however in the present model the only context in which the DH makes a privacy concession is when it accepts the incentive motivation proposed by the DR. Therefore the two events are the same, and their probabilities coincide. We thus can set $p_{op} := p_{priv} = p_{inc}$. Then, the overall objective of the game is to maximize the function:

$$U_{pl}(p_{op}) = (1 - L(p_{op})) * G(p_{op}) \text{ for all } p_{op} \in [0, 1]$$

B. Equilibrium solution

The equilibrium of the game is found by solving the following optimization problem:

$$p_D := \text{Argmax } \{U_{pl}(p_{op})\,;\, p_{op} \in [0, 1]\} \quad (1)$$

that is p_D is the value of p_{op} maximizing the utility function and thereby, reflecting the optimal probability of disclosing private data. Observe that the optimum, p_D can be derived explicitly in the particular case where $g_{priv} = g_{inc}$ and $h_{inc} > h_{priv}$. In the general case we retrieve the value of p_D numerically (figure 12).

C. Strategies

1) Assumptions: We suppose that the following assumptions are reasonable in IoT context-based applications:

- The current context is only observable by DH.
- DR can only deduce the context based on the modified sensing data.
- Previous action results are included in the system.
- DH can only predict the DR strategy from previous action results, which are observable by him/her.
- DH knows in which context the requester has launched its request/attack (curious or malicious).
- DR has the same probability to be curious or malicious.
- The game evolution depends on the negotiation steps between DR and DH based on incentive motivation and privacy preferences.

Parameter	Description
U_{pl}	Utility function of a player pl
L	Loss function (privacy concession)
G	Gain function (incentive motivation)
g_{priv}	Privacy user preference parameter
g_{inc}	Incentive motivation value parameter
h_{priv}	Center of the sigmoid function (loss function)
h_{inc}	Center of the sigmoid function (gain function)
p_{priv}	Probability of making privacy concession by DH
p_{inc}	Probability of accepting the incentive motivation proposed by DR
p_{op}	Equilibrium probability
p_D	Probability of disclosing in the first scenario
p_R	Probability of rejecting in the first scenario
p'_D	Probability of disclosing in the second scenario
p'_R	Probability of rejecting in the second scenario
p	Probability of solving comm. facilities deficiency
l	Probability of having comm. facilities deficiency in the beginning of the game
e	Cost of each game iteration (N and AD states)
c	Probability of having comm. facilities deficiency in the end of the game
p_i	Probability of the final state i.

TABLE IV
GAME PARAMETERS.

2) Decision parameters: Game strategies are described by transitions between states and depend on four parameters: (1) energy and communication facilities, (2) data privacy concession, (3) incentive motivation, and (4) attack/intrusion. For convenience, we summarize notations used in the game formulation in table IV.

3) State transitions: Markov chains are commonly used to represent discrete events random systems, in discrete time, under the assumption that at any time, the distribution of the next state depends only on the value of the random input, and of the current state. For our model the Markov representation has the following state-space:

$$S = \{W, D, R, OoP\} \cup \{(N, i) : i = 0, 1, 2, ...\} \cup \{(AD, j) : j = 0, 1, 2, ...\}.$$

Where W stands for *wait*, D for *disclose*, R for *reject* and *Oop* for *Out of Process* (table V). Any state of the form (N, i) is interpreted as "the agent has been negotiating for i time epochs", and likewise for any state of the form (AD, j), where AD stands for "Attacking/Defending". The game tree is illustrated in figure 3 where we distinguish the two different scenarios explained in IV-B. In each case, DR may iterate the

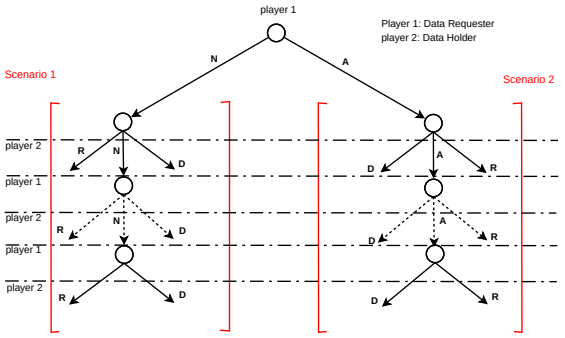


Fig. 3. Sequential game tree.

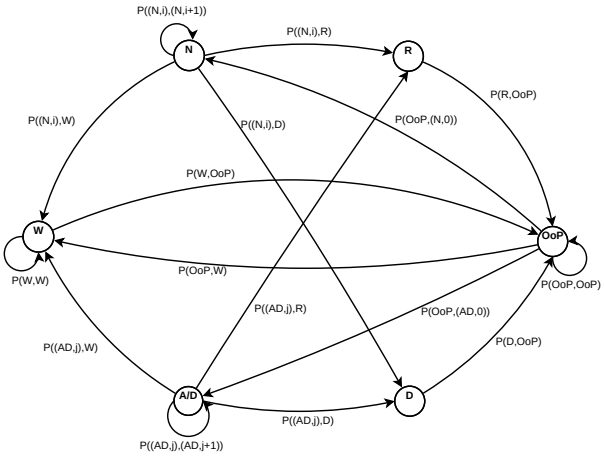


Fig. 4. State diagram representations of the game.

N state, or the AD state until reaching a satisfying agreement (disclose or reject).

Figure 4 presents the state diagram of the Markovian game, and transitions between states. For example, the game player remains in W state in case of communications facilities deficiency, and moves to OoP state otherwise. From OoP state, player can move to N state or to A/D state, and then to D or R states. D and R states leads imperatively to OoP state to begin a new game or to move to W state due to communications facilities constraints. We let e be the energy cost of each iteration of N/AD ($e \ll 1$). c, l, and p are positive reals in $[0,1]$ expressing communications facilities features. Let D and R denote the states "disclose" and "reject"

State	Description
W (wait)	The player is waiting for communication facilities improvement.
OoP (Out of Process)	Communications facilities are favorable and the player is ready for playing.
N (negotiate)	DH and DR negotiate for buying/selling private data.
A/D (attack / defend)	Both players participate in an attack/defense process to access/protect private data.
D (disclose)	DH chooses to disclose private data.
R (reject)	End of the game by rejecting DR demand.

TABLE V
MARKOVIAN PROCESS STATES.

respectively. We assume that p_D and p_R, i.e. respectively the probability of disclosing and rejecting in the first scenario, whenever these actions are possible, are obtained *via* the optimization scheme below. Namely, p_D solves (1) and p_R is such that $p_D + p_R = 1$. Similarity, we define p'_D and p'_R, respectively the probability of disclosing and rejecting in the second scenario ($p'_D + p'_R = 1$). Then, the non-zero terms of the transition matrix are given by:

$$
\begin{aligned}
& P(W,W) = 1-p, \qquad P(W,OoP) = p; \\
& P(D,OoP) = 1, \qquad P(R,OoP) = 1; \\
& P(OoP,W) = 1-c, \qquad P(OoP,(N,0)) = \frac{c}{4}; \\
& P(OoP,(AD,0)) = \frac{c}{4}, \qquad P(OoP,OoP) = \frac{c}{2}; \\
\forall i, \quad & P((N,i),W) = l + ie; \\
& P((N,i),(N,i+1)) = \frac{1}{i+2}; \\
& P((N,i),D) = p_D\left(1 - l - ie - \frac{1}{i+2}\right); \\
& P((N,i),R) = p_R\left(1 - l - ie - \frac{1}{i+2}\right); \\
\forall j, \quad & P((AD,j),W) = l + je; \\
& P((AD,j),(AD,j+1)) = \frac{1}{j+2}; \\
& P((AD,j),D) = p'_D\left(1 - l - je - \frac{1}{j+2}\right) \\
& P((AD,j),R) = p'_R\left(1 - l - je - \frac{1}{j+2}\right).
\end{aligned}
$$

In practice, we assume that the player can be in the states N and AD only for a finite number of times epochs. Specifically, we let i_s and j_s be two positive integers, and allow the states (N,i) only for $i = 0,...,i_s$, and the states (AD,j) only for $j = 0,...,j_s$. This practical assumption makes the state-space of the Markov chain finite. Observe that the events $\{\text{The Chain is in state } (N,i)\}$, $i = 0,...,i_s$ form a partition of the event $\{\text{The agent negotiates}\}$ (and likewise for AD states), we have:

$$
\pi(N) = \sum_{i=0}^{i_s} \pi((N,i)); \ \textit{and} \ \pi(AD) = \sum_{j=0}^{j_s} \pi((AD,j)). \tag{2}
$$

Let us define:

$$
\begin{aligned}
p &:= (p_1,p_2,p_3,p_4,p_5,p_6) \\
&:= (\pi(W),\pi(N),\pi(AD),\pi(D),\pi(R),\pi(OoP)) \\
&= \left(\pi(W), \sum_{i=0}^{i_s}\pi((N,i)), \sum_{j=0}^{j_s}\pi((AD,j)),\pi(D),\pi(R),\pi(OoP)\right)
\end{aligned}
$$

Thus we have:

$$
p_1 + p_2 + p_3 + p_4 + p_5 + p_6 = 1
$$

As the chain is ergodic, p_1 is the long-run proportion of time when the agent is waiting, p_2 is the long-run proportion when the agent negotiates, and so on.

VI. Numerical results

A. Simulations parameters

In table VI, we summarize the simulation parameters used to evaluate the proposed game model. Let p be the probability of the intelligent object to solve communication facilities deficiency. To highlight the effect of its ability to overcome IoT difficulties (battery charging, channel communication channel finding, etc.), we make different simulations for variable values of p as shown in figure 7. Otherwise, we assume that intelligent object is able to solve its communication facilities difficulties, and we fix $p = 0.8$. With l, we expresses the probability of facing communication facilities deficiency by the intelligent object and moving the W state as shown in figure 5 and 6. Otherwise, we suppose that communication facilities conditions are favorable, which means that the value of l is relatively low (we fix $l = 0.1$). The parameter e highlights the cost of each game iteration (N and AD states) as shown in figure 9. It highlights the impact of the game evolution on the communication facilities available to the intelligent object (number of allowed game iterations). By default, we fix $e = 0.1$ which is a realistic value regarding IoT conditions. With c, we indicate the probability of having communication facilities deficiency in the end of the game (transition from *Oop* to W state) as illustrated in figure 8. In favorable conditions we choose $c = 0.9$, and in severe conditions $c = 0.1$. As explained in the previous section, parameters p_D and p_R define respectively the probability of disclosing and rejecting in the first scenario ($p_D + p_R = 1$), while p'_D and p'_R are respectively the probability of disclosing and rejecting in the second scenario ($p'_D + p'_R = 1$). In a first step, we make the simulations for different values of p_D (figures 5, 7, 8, and 9), and p'_D (figure 6) to find the steady state and show the system convergence. In a second step, we calculate the game equilibrium solution numerically based on the utility functions behaviors (L and G) to find the probability of disclosure intention (p_D), as presented in figure 12 and re-inject it in the system state.

Finally, g_{priv} and g_{inc} are respectively the normalized incentive motivation value and privacy user preference parameters. In figure 12, these parameters are used to show the impact of the compromise "user preference/incentive motivation" on the final state of the game. For example, for high value of incentive motivation, the DH has a high probability of disclosure intention (p_D is higher than 0.5). h_{priv} and h_{inc} are the centers of the sigmoid functions, and we choose by default $h_{priv} = h_{inc} = 0.5$.

Simulation parameters	Description
p	Probability of solving comm. facilities deficiency
l	Probability of having comm. facilities deficiency in the beginning of the game
e	Cost of each game iteration (N and AD states)
c	Probability of having comm. facilities deficiency in the end of the game
p_D	Probability of disclosing in the first scenario
p_R	Probability of rejecting in the first scenario
p'_D	Probability of disclosing in the second scenario
p'_R	Probability of rejecting in the second scenario
g_{priv}	Privacy user preference parameter
g_{inc}	Incentive motivation value parameter
h_{priv}	Center of the sigmoid function (loss function)
h_{inc}	Center of the sigmoid function (gain function)

TABLE VI
Simulation parameters.

B. Steady state

We remind that the player switches from other states to W state in case of energy limitations problem. The player's behavior, when this phenomenon occurs, is reflected by parameter l which expresses the default value of energy consumption in sleep situation, and parameter e, which handles energy consumption in each iteration of N or AD states. Once the player is in state W, he/she leaves only when communication facilities problems are solved. In addition, the player lasts in state OoP when he/she is not facing any communication problems, but waiting for "something to happen" (starting a game spontaneously, or waiting for a game proposal from another player).

Steady states for $i_s = 3$ and $j_s = 3$ are shown in figures 5, 6, 7, 8, and 9. In each sub-figure, we fixed p, c, l, e, p'_D and p'_R, and calculate the steady state probabilities for 5 increasing values of p_D and p_R (from 0.1 (left bars) to 0.9 (right bars)). Similarly, in figure 6, probabilities are calculated for 5 increasing values of p'_D and p'_R.

In figure 5, we choose $p = 0.8$, $c = 0.9$ and $e = 0.1$ which means that the player is not facing any communication facilities problem at the beginning of the game. For small values of l, the player stays a shorter period of time in W state than OoP state. That means, from the communications facilities point of view, the player can freely play and no constraints are inhibiting his/her behavior. In addition, time spent in N, AD, D and R states is high since the player is active and has the possibility to make decisions. In return, for big values of l, the player lasts more time in W state as energy consumption is high. We notice that numerical values of the game result D and R are around 10%, which is explained by their shortness in real time. In figure 6, we used the same logic to show the steady state values in attack scenario. The main difference is that, if we assume the existence of defense mechanisms, the probability of disclosing private data is clearly lower than the probability of rejecting the DR demand. For the rest of parameters, which depend only on communication facilities, players behaviors are similar to those in figure 5. In figure 7, we focus on the impact of parameter c in severe situation of constraints ($c = 0.1$). Even for low energy consumption ($e = 0.1$) high value of p and low

Fig. 5. Steady state for variable l, p_D and p_R.

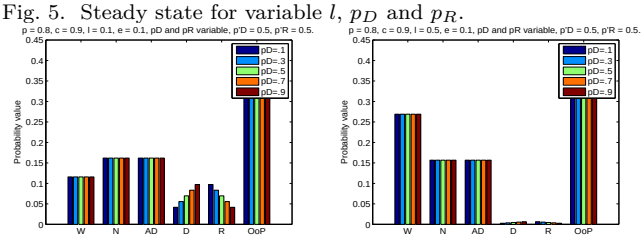


Fig. 6. Steady state for variable l, p'_D and P'_R.

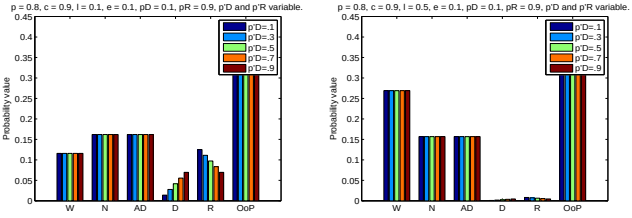


Fig. 7. Steady state for variable p, p_D and P_R.

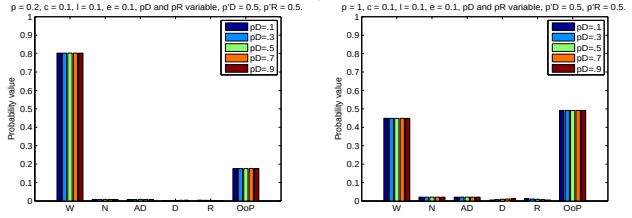


Fig. 8. Steady state for variable c, p_D and P_R.

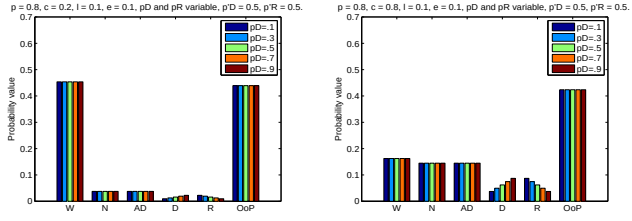


Fig. 9. Steady state for variable e, p_D and P_R.

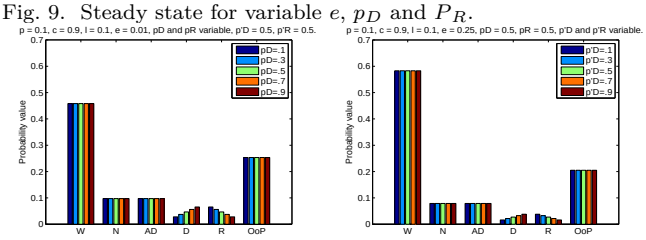
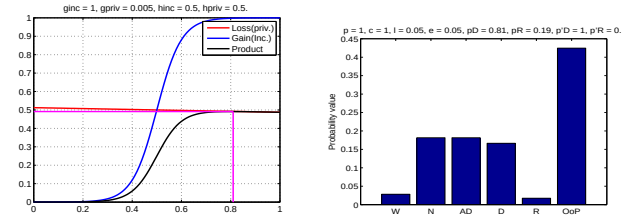


Fig. 10. Steady state for particular ITS case.



(a) Equilibrium (b) Steady state probabilities

value of l, the game player lasts very short period of time in active states: N, AD, D and R. To avoid inactivity situation perceived in figure 7, we fixed $p = 0.8$, $l = 0.1$, $e = 0.1$ and $p_D = p_R = 0.5$ in figure 8, and we did the steady state calculation for different values of parameter c. As we explained previously, for small values of c, the player has communication difficulties and lasts long period of time in W state. For high values of c, the player participates actively in the game and lasts more time in OoP, N, AD, D and R states than W state. In figure 9, we focus on the energy cost of N and AD states. If they are costly, time spent in active states (OoP, N, AD, D and R) decreases, otherwise it increases.

C. Equilibrium

We solve the game equilibrium for different situations in the game numerically. Then, we represent gain function and loss function, calculate their product, find their maximum point, and get the corresponding steady state. To distinguish between different situations, we modify the normalized value of parameters g_{inc} and g_{priv}, and analyze the player's behavior (figure 12). For a limited privacy concession ($g_{priv} \ll 1$), we search for the equilibrium point for different values of g_{inc}. We notice that the probability of disclosing data is high ($p_{op} > 0.5$). For an intermediate privacy concession ($g_{priv} = 0.5$), we found that equilibrium probability for small values of g_{inc} (non interesting incentive motivation) is small. That means, disclosing private data for the high values of g_{inc} is more probable due to the interesting incentive offer ($p_{op} \approx 0.2 - 0.6$). If we choose a high privacy concession ($g_{priv} \approx 1$), we find that equilibrium probability for different values of g_{inc} (interesting and non interesting incentive motivation) is low. That means, players hesitate to disclose private data even for high values of g_{inc} ($p_{op} < 0.5$) in almost all situations.

To compare our contribution to other proposals, we consider three different research papers [27] [11] [28] and we run simulations as shown in figure 11. Results of comparison are explained in the following. In [27], authors proposed a differential privacy solution for anonymization and correlated privacy preserving analysis in big data. They used a truncated geometric mechanism (TGM) to illustrate the dynamic privacy choices, and ln function to fit the relationship between utility and privacy. The expected payoff is represented in black ($F(s) = \alpha_1 ln(s + \alpha_2) + \alpha_3$; $s > 0$), and is calculated for $\alpha_1 = 0,05811$, $\alpha_2 = 0,001$, $\alpha_3 = 0,7652$. In [11], authors proposed an infinite repeated game for privacy protection in mobile application. They introduced a discount coefficient that discounts future earnings to weigh the pros and cons of different paths. The user tries to maximize his utility by

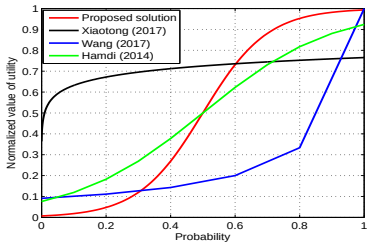


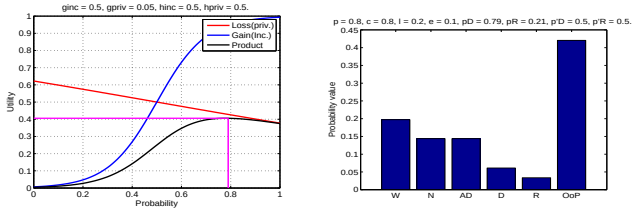
Fig. 11. Utility functions comparison.

controlling the probability of releasing his private data, and when the discount coefficients satisfy the ranges, the player loses the motivation to actively deviate from the social norm. The expected payoff is represented in blue ($U_{ui}(c) = Q(c)/1 - \delta_u$; $0 \leq \delta_u \leq (1)$), and is calculated for $Q(c) = 2$. In [28], authors proposed damage and lifetime functions to calculate player's benefits. We model the opposite of their damage function $(1-\Delta)$ in function of $(1-P_{pv})$, which is a correct representation of data disclosure (green curve). Compared to our solution, the two function have similar behaviors but gain values depends on data privacy *vs* incentive motivation in our case. For example, in figure 11 for low probability of disclosure intention, the gain of their solution is higher than our proposed solution, which can be explained by the value of the sigmoid function's steepness. In our proposal, we adapt the gain value in function of incentive motivation to show its impact on DH's disclosure intention and equilibrium solution. In addition, we study the balance between incentive motivation and privacy concession by inserting the latter parameter in loss function to analyze the final state of the game. That means, for high values of g_{inc}, the gain value is high, and for high values of g_{priv}, the loss value is high, and vice versa.

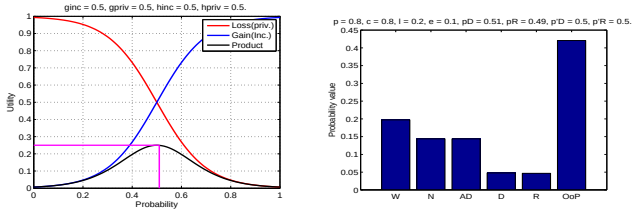
D. ITS Particular case

In ITS, we need to consider particular cases where DR is the authority representative, the public safety, or emergency management applications. In these situations, response of DH has to be instantaneous with the required aid. Our model provides flexibility to solve this problem by adjusting some precise parameters. Then, we fix $p = c \approx 1$ (no communications constraints exist), $l = e \approx 0$ (energy consumption is low), and $p'_D = 1$ (no resistance of disclosing data is shown) as shown in figure 10. We notice that $p_D = 0.81$ which reflects a high disclosure intention, which is confirmed by the steady state probabilities ($\pi(D) \gg \pi(R)$). We also notice that time spent in OoP state is much higher than W state, which highlights the readiness of the DH to answer the DR request in this type of situations.

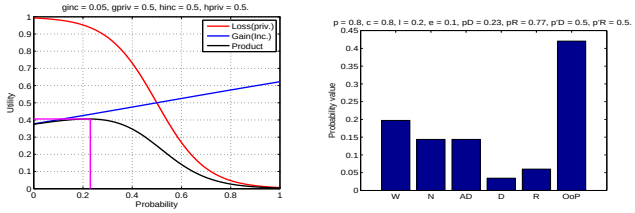
Fig. 12. Game equilibrium and steady states for normalized values of incentive motivations and privacy concession.



(a) High incentive, low privacy concession



(b) Medium incentive, medium privacy concession



(c) Low incentive, high privacy concession

VII. Conclusion and future work

In this paper, we proposed a Markovian game-based solution to protect private data exchanged in the ITS context where each player aims to maximize his/her payoff. This approach can be used during negotiation between actors to predict the DR's strategies, and then to determine the DH's decisions based on the compromise found in the equilibrium solution between privacy concession and incentive motivation. Our model considers two different scenarios (DR: curious or malicious), and is applicable in particular cases of ITS by adapting its parameters. With this aim in mind, we defined six different states for each player, solved the Markovian system numerically, and illustrated the steady state. We come up to integrate parameters related to IoT context and those related to privacy preservation in a global system. Then, we sketched the DH behavior in different situations by adapting the corresponding parameters of the system such as energy costs, privacy concession and incentive motivation. Finally, we illustrated the utility function to analyze the equilibrium solution of the system, which reflects the disclosure probability of DH, p_D. This parameter is calculated to illustrate the DH ability to disclose private data in each situation by adapting energy, incentive and privacy parameters. Then, we showed that DH behavior depends to its current situation and acts accordingly.

In the future, we will focus on long-term players payoffs (after many game instances) and their effect on the game continuity (final states and transition). Also, we will consider new players behavior and types, and generate and analyze new models accordingly.

References

[1] W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, and X. Shen, "Internet of vehicles in big data era," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 19–35, Jan 2018.

[2] X. Liang, K. Zhang, X. Shen, and X. Lin, "Security and privacy in mobile social networks: challenges and solutions," *IEEE Wireless Communications*, vol. 21, no. 1, pp. 33–41, February 2014.

[3] A. Blume, Y.-G. Kim, and J. Sobel, "Evolutionary stability in games of communication," *Games and Economic Behavior*, vol. 5, no. 4, pp. 547–575, 1993.

[4] D. A. Meyer, "Quantum strategies," *Physical Review Letters*, vol. 82, no. 5, pp. 1052–1055, February 1998.

[5] D. A. Meyer and T. A. Brown, "Statistical mechanics of voting," *Physical Review Letters*, no. 81, pp. 1718–1721, June 1998.

[6] Y. Li, F. Liu, and A. S. Morse, "A distributed, dynamical system view of finite, static games," in *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Oct 2017, pp. 732–738.

[7] P. Bichsel, J. Camenisch, B. D. Decker, J. Lapon, V. Naessens, and D. Sommer, "Data-minimizing authentication goes mobile," in *Communications and Multimedia Security - 13th IFIP TC 6/TC 11 International Conference, CMS 2012, Canterbury, UK*, September 2012, pp. 55–71.

[8] M. Milutinovic, I. Dacosta, A. Put, and B. D. Decker, "ucentive: An efficient, anonymous and unlinkable incentives scheme," in *2015 IEEE TrustCom/BigDataSE/ISPA, Helsinki, Finland, Volume 1*, August 2015, pp. 588–595.

[9] P. Verhaeghe, K. Verslype, J. Lapon, V. Naessens, and B. D. Decker, "A mobile and reliable anonymous epoll infrastructure," in *Security and Privacy in Mobile Information and Communication Systems - Second International ICST Conference, Catania, Sicily, Italy, Revised Selected Papers*, May 2010, pp. 41–52.

[10] I. Wagner and D. Eckhoff, "Technical privacy metrics: a systematic survey," *CoRR*, vol. abs/1512.00327, 2015.

[11] E. A. Panaousis, A. Laszka, J. Pohl, A. Noack, and T. Alpcan, "Game-theoretic model of incentivizing privacy-aware users to consent to location tracking," *CoRR*, vol. abs/1601.00167, 2016.

[12] Y. He, L. Sun, W. Yang, and H. Li, "A game theory-based analysis of data privacy in vehicular sensor networks," *IJDSN*, vol. 10, 2014.

[13] J. Li, J. Yang, Y. Zhao, B. Liu, M. Zhou, J. Bi, and Q. Wang, "Enforcing differential privacy for shared collaborative filtering," *IEEE Access*, vol. 5, pp. 35–49, 2017.

[14] F. Wang, N. Zheng, D. Cao, C. M. Martinez, L. Li, and T. Liu, "Parallel driving in cpss: A unified approach for transport automation and vehicle intelligence," *IEEE CAA Journal of Automatica Sinica*, vol. 4, no. 4, p. 577, 2017.

[15] Z. Tan, C. Wang, M. Zhou, and L. Zhang, "Private information retrieval in vehicular location-based services," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Feb 2018, pp. 56–61.

[16] A. Devare, A. Hande, A. Jha, S. Sanap, and S. Gawade, "A survey on internet of things for smart vehicles," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 5, no. 2, pp. 1212–1217, 2 2016.

[17] J. Petit, M. Feiri, and F. Kargl, "Revisiting attacker model for smart vehicles," in *IEEE 6th International Symposium on Wireless Vehicular Communications, WiVeC 2014*. Piscataway, NJ, USA: IEEE, September 2014, pp. 1–5.

[18] R. Currie, "White paper: Developments in car hacking," SANS Institute, InfoSec Reading Room, US, Tech. Rep., January 2016.

[19] J. Katz, *Bridging Game Theory and Cryptography: Recent Results and Future Directions*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 251–272.

[20] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: A survey." *CoRR*, vol. abs/1610.06095, 2016.

[21] Y. Dodis and T. Rabin, *Cryptography and game theory*. Cambridge University Press, 1 2007, pp. 181–206.

[22] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, "A systemic approach for iot security," in *DCOSS*. IEEE, 2013, pp. 351–355.

[23] A. Riahi, E. Natalizio, Y. Challal, N. Mitton, and A. Iera, "A systemic and cognitive approach for IoT security," in *International Conference on Computing, Networking and Communications (ICNC 2014)*, Honolulu, USA, 2014, invited Paper.

[24] A. S. Riahi, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the internet of things," *Digital Communications and Networks*, 2017.

[25] P. Papadimitratos, A. de La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation." *IEEE Communications Magazine*, vol. 47, no. 11, pp. 84–95, 2009.

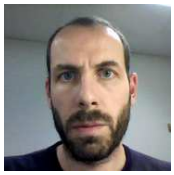
[26] D. Niyato, D. T. Hoang, N. C. Luong, P. Wang, D. I. Kim, and Z. Han, "Smart data pricing models for the internet of things: a bundling strategy approach," *IEEE Network*, vol. 30, no. 2, pp. 18–25, 2016.

[27] X. Wu, T. Wu, M. Khan, Q. Ni, and W. Dou, "Game theory based correlated privacy preserving analysis in big data," *IEEE Transactions on Big Data*, vol. abs/1512.00327, 2017.

[28] M. Hamdi and H. Abie, "Game-based adaptive security in the internet of things for ehealth," in *IEEE International Conference on Communications, ICC 2014, Sydney, Australia, June 10-14, 2014*, 2014, pp. 920–925.

Arbia RIAHI SFAR is Associate Professor, and a member of VRIT laboratory, at the Military Academy of Foundouk Djedid (Tunisia). She has received the PhD degree in computer science from Compiègne University of Technology in France, and Tunis Polytechnic School in Tunisia. Her research interests include communication security and privacy in Internet of Things (IoT).

Yacine CHALLAL is ....



Pascal MOYAL is Full Professor in Applied Mathematics at Université de Lorraine. His research activities are mostly devoted to the study of Stochastic Processes and their applications. In particular, Weak Approximations (fluid and diffusion limits) of Queuing systems and Stochastic Networks; Convergence of Random Graphs and applications to Epidemiology and Wireless Networks; Stochastic matching problems on graphs; and Stability of Stochastic Recursions (Ergodic Theoretical approach).

Enrico NATALIZIO (Member IEEE) is Full Professor at Université de Lorraine. His research interest include robot&sensor communications with applications in networking technologies for disaster management and infrastructure monitoring, as well as IoT privacy and security. He is currently an associated editor of Elsevier Ad hoc Networks, Elsevier Digital Communications and Networks and Wiley & Hindawi Wireless Communications and Mobile Computing.