# A Markov game privacy preserving model in retail applications

Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, Zied Chtourou

# A Markov game privacy preserving model in retail applications

Arbia Riahi Sfar*, Enrico Natalizio*, Yacine Challal†, Zied Chtourou‡,
* Sorbonne universites, Universite de Technologie de Compiegne, CNRS, Heudiasyc UMR 7253.
e-mail: *name.lastname*@hds.utc.fr
† Laboratoire de Methodes de Conception de Systemes (LMCS), Ecole Nationale Superieure d'Informatique (ESI), Centre de Recherche sur l'Information Scientifique et Technique (CERIST) Algiers, Algeria. e-mail: y_challal@esi.dz
‡ VRIT Lab - Military Academy of Tunisia, Nabeul, Tunisia. e-mail: ziedchtourou@gmail.com

***Abstract*—New retail applications induce integration of many components as NFC (Near Field Communication), M2M (Machine-to-Machine), IoT (Internet of Things), Web applications, etc. in large business sectors, such as payment services, products manufacturing, supply chain management, etc. Sensors, integrated in everyday products may facilitate threats as users tracking and profiling. An increasing concern about privacy threats posed by data affluence and device ubiquity takes place. This paper presents a privacy scheme for retail applications, discusses challenges related to customer profiling, client consent, device and information security. To protect customers' data, we propose a Markovian game, with detailed states, actions, strategies and transitions available for data holder to reach a compromise between privacy concessions and incentive motivation proposed by data requester. Numerical results are used to analyze and evaluate the game theory-based model.**

***Keywords*—Retail application, privacy, game theory, Markovian process.**

## I. Introduction

In the retail market, the Compound Annual Growth Rate (CAGR) of IoT devices is expected to grow of 20% between 2015 and 2020[1]. New applications ameliorate in-store activities of retailers using smart barcode scanners, mobile payment systems and product recommendations. Data related to user preferences collected by connected devices may be used by retailers to trace fast moving items, replace less preferred items with popular items and guide faster and increased sales.

Thanks to their low power consumption, connected devices (RFID, Zigbee, BLE and NFC devices, etc.) in recent retail solutions are subject to an uninterrupted evolution during the last few years. New opportunities have been created to establish new activities and practices in our everyday life. This development persuades retail giants such as Walmart to invest powerfully in novel technologies by designing solutions to accept any payment type with almost any smartphone [1]. This evolution invokes massive possibilities for exchanging private data through new business models across manufacturers, suppliers, and products and service providers. Making relevant technologies secure and reliable becomes the basis to carry out this concept development.

In retail scenarios, it becomes vital to investigate and understand privacy implications and create new policies for relationship between consumers and their data in the real world [2]. These aspects include communication compromising, customers agreement, data anonymity, data access control. Questions related to intelligent objects identification (devices' owners), location (device's location, owner's location), search query (profiling the owner based on his/her ordered items) and digital footprint (traceable data on the internet) need to be answered [3].

Although privacy is a key topic in these applications, there are not enough studies and research efforts about preserving data privacy. For example, consumers need to be aware that their privacy can be affected by online networking of a huge number of connected objects, systems and humans.

Unfortunately, many connected devices are known for their limited memory space and computational capabilities. Then, conventional privacy solutions as encryption methods, and other security systems as firewall, are inadequate to solve the challenging privacy concerns [4]. One promising solution is the use of game theory to model the interactions of actors and decision challenges in privacy scenarios. The large number of mathematical tools available for multi-user strategic decision making seems to be a catalyst factor.

In this work, we focus on new retail applications where data privacy protection is a challenging issue. We propose a privacy preservation model between data holder (consumer devices) and data requester (manufacturer, supplier, etc) based on game theory, to find the optimal protection strategy and preserve private data over a series of interactions with a data requester. Our contribution is twofold: (1) we present a general context of a retail applications, discuss privacy challenges, and (2) we propose a game theory-based model to solve privacy problems based on a Markovian process.

*This work has been carried out in the framework of the Labex MS2T, which is funded by the French Government, through the program 'Investments for the future', managed by the National Agency for Research (Reference ANR-11-IDEX-0004-02).

[1]https://www.einfochips.com/blog/solution/internet-things/top-5-trends-in-iot-for-2016.html

The remaining of this paper is organized as follows. Section II depicts the most important research activities dealing with the use of game theory to solve security and privacy questions in retail applications. Section III presents the context of our work and shows actors of retail solutions. Section IV focuses on actors, roles, game parameters and strategies. Sections V and VI detail the game model and analyze its properties through numerical results. The last section concludes the paper and proposes possible future directions.

## II. Related work

Game theory deals with interactions within specified rules of play and different choices. Thanks to to its mathematical rigor, many researchers choose to use this concept in formulating interactions between actors in security scenarios [5]. To the best of our knowledge, research activities related to privacy protection in retail context using game theory are still very limited. In [6], authors developed a non-cooperative game-theoretic framework that captures the structure of the American supermarket industry and show observed behavior for supermarket chains within this industry. Despite the innovation brought by the proposed approach in the economical field, security and privacy concerns were not discussed in their work. Thus, risks of private data attacks remain unsolved, and even not considered. In [7], authors proposed a stochastic game model to determine the best strategy to be applied by banks for ATM services extension. They also provided an algorithm to identify the idle locations where a bank should place an ATM based on the result of the ATM game recommendation. Although the sensitivity of exchanged data across many networks and infrastructures, authors of this work did not discuss privacy risks, and did not provide any solution.

As privacy protection in retail context using game theory is not seriously handled in other research activities, we are encouraged to debate this issue and propose a game theory based model to protect private data. Since stochastic games are widely used to model interactions between malicious attackers and defenders [8], we adopt this principle to deal with privacy concerns. Their strength is the ability to capture interactions between players and dynamics of the overall system. This is quite helpful to compute probabilities of an expected adversary behavior, to build a transition matrix between system states, and to evaluate security in an interconnected system.

## III. Retail application and privacy preservation

In retail applications, connected objects permit producers to receive real-time information about product use and consumer traditions. These information may be exploited to ameliorate production and modify/remove the unused products, which improves their roadmap to direct future consumer acquisitions [9].

As the number of embedded devices that require mobile connectivity grows, retail stakeholders are expected to be big contributors to this rapidly emerging and complex ecosystem. The key of success in these situations is to handle efficiently a big amount of data, that may contain sensitive information about individual's habits. An increasing concern about privacy menaces provoked by data abundance and device ubiquity takes place. For example, individuals have to be sure that their data, collected for a specific purpose, are not reused for another purpose without their permission.

to solve privacy issues in practice, two solutions are possible: privacy by design, and privacy enhancing technologies [10]. Privacy by design is considered at the beginning of the development of a product, a service or a system, and handles the integration of privacy protection into both technology (computer chips, networking platforms, etc.) and organizational policies (privacy impact assessments). Privacy enhancing technologies avoid personal data compromise, rebuild trust between users and service providers, and consider the dimension and emerging big data environment. Possible techniques to preserve privacy are listed in [10] and include anonymization, encryption, security and accountability controls, transparency, consent, ownership, and control. However, authors deduce that the road to protect big data privacy is still long, as generated data are growing every day, and privacy preserving mechanisms development is still time-consuming.

Lately, game theory has emerged as a method for modeling interactions between numerous rational selfish entities with conflicting interests, and for calculating stable system points (equilibrium) from which no entity can obtain additional benefit [11]. In [5], a comprehensive survey on security and privacy in computer and communication networks using game-theoretic methods is provided. Depending on the nature of available information, players behaviors, possible actions and final goals, many types of security games can be distinguished as simple deterministic, zero-sum, Stackelberg, repeated, stochastic, and incomplete information.

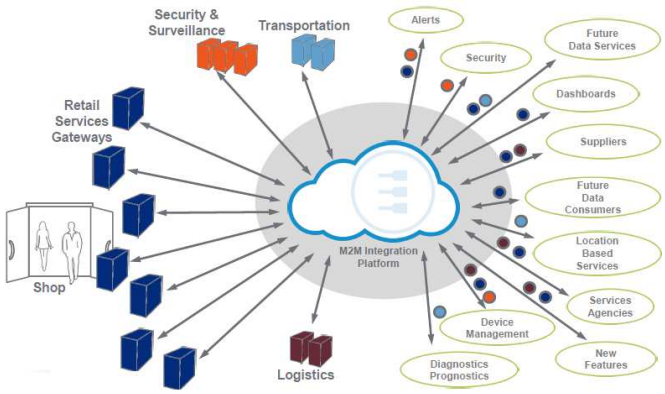


Figure 1. Retail automation and integration [12].

In Figure 1, the different actors and interactions of a retail scenario are shown. Private data are hold by intelligent objects connected to physical products and consumer smart applications. For example, we consider the scenario of analyzing interactions between customer

purchases and stores. The retailer has the possibility to use purchase data to identify customers preferences, and to better serve them and increase his/her revenues. In this scenario, to understand customer's behavior and affinity, and to improve marketing and promotions in specific trade areas around each store, many aspects need to be considered as customer's opinions, closeness to a store, etc.

Intelligent objects are tightly related to consumer, and play the role of private data holder (DH) in the game. Supply chain management, inventory management, e-commerce service providers and many other actors are interested in these data to model the consumer behavior and develop their services accordingly. To motivate consumers to disclose their private data, data requester (DR) propose incentive motivation to convince DH to accept privacy concession. To reach a final compromise, this operation (called negotiation) may take place in many steps. The final decision is taken by DH who may accept or refuse to disclose private data.

## IV. Game description

Application of game-theoretic approaches to the interactions among users of a retail application can be modeled as a game for the following reasons. First, we assume that players are rational, know the full structure of the game, and DHs grant high interests in privacy preservation of their data. Second, each player's benefit depends on the other player's strategy and decision. Third, taking into account incentives of the players, and the usage of an adequate game strategy, may lead DH to get useful implications on adversary behavior and increase player's outcome. Finally, we can provide players with the convenient decision making mechanism to assure a minimal damage happening.

### A. Actors and roles

Actors and roles in our game are presented in Table I. DH stores private information, whereas DR aims at accessing these data by proposing incentive motivation.

Table I. Players, actions and payoffs of the game.

| Player | Actions | Payoffs | Implications of equilibrium |
|---|---|---|---|
| DR | Wait (W).<br>Requests access to private data (R).<br>Chooses an incentive paid for DH (N).<br>Stop the game (OoP). | **Income**: access to private data.<br>**Expense** : incentives paid to DH. | Players are satisfied with final values of data privacy and incentive motivation. |
| DH | Wait (W).<br>Reply the request (R).<br>Negotiate incentive value (N).<br>Disclose private data or reject (OoP). | **Income**: incentives received from DR.<br>**Expense**: privacy loss of sensitive data. | |

We are aware that it is difficult, for a person, to distinguish if a data is sensitive or not and what will be the outcome after exposing the data. In our work, we consider the substantial work of others researchers to deal with this question. In [13], authors dealt with information literacy, which concerns familiarity with technical features, and awareness of privacy practices and rules, and discussed means of managing digital identities by people. In [14], authors considered privacy as a compromise between individuals choice and online services. They used everyday Internet data to investigate how individuals integrate online activities in their daily lives, and suggested three organizing "moments" of online privacy perceptions: (1) sitting in front of the computer, (2) interacting with it, and (3) after releasing data in the Internet. In [15], authors proposed to contextualize individual privacy activity online, in contact with political, social and economic environments. This concerns private information economy, which is guided by governments, and constituting the target of a growing market for personal data.

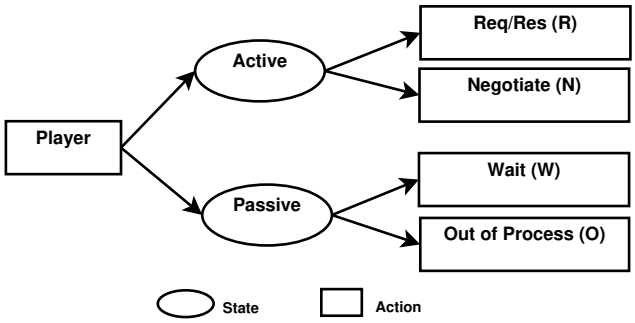


Figure 2. States and actions of DH.

Once privacy preferences are defined by DH for one data record, it is meaningful to answer how DHs may define the privacy preferences of all data. And, if the exposure of every data need to inquire users, will the applications be limited due to the extremely high latency caused by human interactions. In [16], authors examined the evolution of IoT and the privacy paradox, and proposed technological and socio-technical research to establish a reasonable equilibrium. An example of a concrete solution is the use of the platform for Privacy Preference (P3P) which has been proposed by W3C as a mean for practicing privacy of web sites [17].

### B. Players states, actions and strategies

*States and actions:* We choose two macro-states for each player: *active*, and *passive*. In the *active* mode, the player participates to the game and may *request/response* access to private data or *negotiate* incentive motivations and privacy parameters. In the *passive* mode, the player refuses to participate in the game (*wait*) by making the decision of disclosing private data or moving $Out\,of\,Process$ by rejecting the request as illustrated in figure 2.

*Strategies parameters:* Each player chooses his/her strategy to switch between states through available actions. For each strategy, we define the transition probabilities between states according to three distinct parameters. The first parameter is related to energy and communication facilities such as battery level, channel

state (good, degraded or absent) and memory state (number of packets in the queue). We assume that all these facilities must be available for any entity to be involved in the proposed game. To simplify ideas, during the game, the node has to be sure if communication facilities are $favorable$ or not by verifying all of the above mentioned facilities. If any of the parameters is unfavorable, the node switches to the passive mode (absence of communication channel, low level of energy, etc.). The second parameter concerns incentive motivation proposed by DR to DH for accessing private data. It depends on external market conditions which indicate how valuable the data is to DH and the incentives value proposed by DR in the negotiation phase. This motivation may influence DH to change his/her initial proposal by making privacy concession. The third parameter handles privacy preferences and concession made by DH. Privacy preferences may be involved, for example, in the case of consumer who can authorize specific actors (other consumer, supplier, etc.) to view or modify their consumption's habit information. The privacy loss of disclosed data may be perceived when DH makes privacy concession by decreasing privacy preferences and disclose his/her private data.

## V. Game model

### A. System components

The objective of our game is to find the optimal defense strategy for a DH to preserve privacy against a DR over a series of interactions with a DR. As DH and the adversary have opposite objectives, their interactions may be modeled as a non-cooperative game. DH may encounter a set of interactions $C = \{c_1, c_2, ....c_n\}$. We adopt the Markovian process to capture the transitions between interactions [18]. It has been shown that human behaviors and activities extracted from intelligent objects (sensors, actuators, etc.) may be modeled after a two-state Markovian process. At time $t$, the user's interaction is denoted as $C_t \in C$, which is generated from a Markov model $M$. According to the independence property of Markovian process:

$$Pr[C_t = ci|C^1, ..., C^{t-1}] = Pr[C_t = ci|C^{t-1}] \qquad (1)$$

We assume that the adversary is able to obtain the released sensing data at the time when the untrusted application accesses the data, and is assumed to know the Markovian process of DH. As the interactions and user's released data privacy vary over the time, the adversary can adaptively maximize its long-term benefit. To protect private data against all types of adversaries, we make the assumption that the adversary is curious and selfish, so he/she aims at minimizing DH's benefit through a series of strategic operations.

### B. Game strategies

*a) State space and interaction features:* DH may or not disclose data of multiple sensors to the DR. Previous action results are included in the system state and DH's action depends on its observation of the current interaction which is possible for him/her. DR may only deduce the interaction based on the modified sensing data and the user's Markov model. As DR's strategy is unknown to DH, he/she may only predict the DR strategy from previous action results, which are assumed to be observable. This assumption is reasonable in interaction-based applications. We also suppose that DR is *curious*, and attempts at accessing private data, which are not accessible in normal situations. So, he/she has to propose an incentive motivation to reach his/her goal.

*b) State transitions/Strategies:* As explained previously, games strategies depend on three parameters: $c$ (energy and communication facilities), $p$ (data privacy) and $i$ (incentive motivation). The game player switches between *passive* and *active* modes according to these parameters. Table II presents conditions probabilites for state transitions. We define $j$ the number of DRs involved in the privacy game, and $k$, an integer satisfying $k \in \{1, ...j\}$.

Table III shows the different strategies available for each player. For example, in strategy 1, the player switches automatically to the active mode if communications facilities are favorable. Otherwise, he/she switches to the passive mode. As the condition "communication facilities favorable" is not always true in dynamic contexts, we assign a probability value to the case where it is satisfied.

### C. State transition graphs

A Markovian process describes the system whose states change over time, commonly called discrete time stochastic process [19]. The probability matrix $P = (P_{ij})$ specifies the transition rules if the size of $S$ is $N$, $P$ is a $N \times N$ stochastic matrix. Every finite state Markov chain has at least one stationary distribution (also called steady state) which satisfies:

$$\begin{cases} \sum_{k \in S} \pi(k) & = 1; \\ \pi P & = \pi. \end{cases} \qquad (2)$$

In our game, DR aims at accessing private data by proposing incentive motivation spontaneously. But, DH has to find a balance between his/her data privacy preferences and financial motivations. As he/she has to make privacy concessions, the strategy choices of DH seems to be more challenging. In figure 3, we present the state diagram from DH's perspective and we show transitions between ations and their impact on player's behavior. Transition conditions and probabilities are given in table IV.

As we mentioned before, to perform any action during the game, three parameters of strategy adaptation have to be considered (communication facilities, privacy adaptation, and incentive motivation). For example, if we consider transition W1, game player will switch from passive state ($wait$) to active state ($request/response$), and has only to consider the first parameter. The other two parameters are not applied in this transition, which explains the probability of this transition.

Table II. Conditions probabilities.

| Conditions | Conditions probability | Description |
|---|---|---|
| Communication facilities | $= \begin{cases} p_c^1 & favorable \\ 1-p_c^1 & unfavorable \end{cases}$ | Communication resources are available or not. |
| Incentive motivation | $= \begin{cases} p_i^1 & max_k(m_k) \geq m_{min} \text{ and } n^t \leq n_{max}^t. & \text{interesting incentive \& max iter. not reached.} \\ p_i^2 & max_k(m_k) < m_{min} \text{ and } n^t \leq n_{max}^t. & \text{non interesting incentive \& max iter. not reached.} \\ 1-p_i^1-p_i^2 & n^t > n_{max}^t. & \text{max iter. reached.} \end{cases}$ | $j$ DRs propose incentive values $\{m_1, m_2, ....m_j\}$, DH decides based on the minimum expected value ($m_{min}$), number of negotiation iterations ($n^t$), and maximum number of iterations allowed ($n_{max}^t$). |
| Privacy concession | $= \begin{cases} p_p^1 & \rho(1-\alpha) \geq p_{min}. & priv.\ concession\ not\ needed. \\ 1-p^1{}_p & \rho(1-\alpha) < p_{min}. & priv.\ concession\ needed. \end{cases}$ | DH decides to make concession based on privacy preferences ($\rho$), level of data disclosure ($\alpha$), probability of the realized data privacy protection ($\beta = 1-\alpha$), and a fixed threshold $p_{min}$. |

Table III. Game strategies of DH.

| Transition | Transition probability | Condition | Condition Probability |
|---|---|---|---|
| Strategy 1 (adapting to the communication facilities): Game player switches to the *passive* mode if one of the parameters among the *communication facilities* is not acceptable, and to the *active* mode if all the parameters are acceptable. | | | |
| Passive →Active | $P_{P\Longrightarrow A} = p_c = \begin{cases} 1 \\ 0 \end{cases}$ | * favorable<br>* unfavorable | $p_c^1$<br>$1-p_c^1$ |
| Active → Passive | $P_{A\Longrightarrow P} = p_c = \begin{cases} 0 \\ 1 \end{cases}$ | * favorable<br>* unfavorable | $p_c^1$<br>$1-p_c^1$ |
| Strategy 2 (adapting to the incentives): Game player switches to the *passive* mode if the market conditions or the proposed incentives are not motivating. We define $0 < p_{inc} < 1$, and $0 < p'_{inc} < 1$, the probabilities of accepting incentive motivation by DH. | | | |
| Passive →Active | $P_{P\Longrightarrow A} = p_i = \begin{cases} p_{inc} \\ 1-p'_{inc} \\ 0 \end{cases}$ | * Interesting incentive motiv. and max iterations num. not reached.<br>* Non interesting incentive motiv. and max iterations num. not reached.<br>* Max iterations num. reached. | $p_i^1$<br>$p_i^2$<br>$1-p_i^1-p_i^2$ |
| Active → Passive | $P_{A\Longrightarrow P} = p_i = \begin{cases} 1-p_{inc} \\ p'_{inc} \\ 1 \end{cases}$ | * Interesting incentive motiv. and max iterations num. not reached.<br>* Non interesting incentive motiv. and max iterations num. not reached.<br>* Max iterations num. reached. | $p_i^1$<br>$p_i^2$<br>$1-p_i^1-p_i^2$ |
| Strategy 3 (adapting to the privacy): Game player switches to the *passive* mode if privacy concession is needed and to the *active* mode otherwise. We define $0 < p_{pr} < 1$, and $0 < p'_{pr} < 1$, the probabilities of changing privacy preferences by DH. | | | |
| Passive →Active | $P_{P\Longrightarrow A} = p_p = \begin{cases} p_{pr} \\ 1-p'{}_{pr} \end{cases}$ | * Privacy concession not needed.<br>* Privacy concession needed. | $p_p^1$<br>$1-p_p^1$ |
| Active → Passive | $P_{A\Longrightarrow P} = p_p = \begin{cases} 1-p_{pr} \\ p'{}_{pr} \end{cases}$ | * Privacy concession not needed.<br>* Privacy concession needed. | $p_p^1$<br>$1-p_p^1$ |

For calculation simplicity, we consider the following new variables: $a = p_c^1[p_{pr}p_p^1 + ((1-p_{pr}^{'})(1-p_p^1)]$, $b = [p_{inc}p_i^1 + (1-p'_{inc})p_i^2]$, $c = p_c^1 p_p^1[(1-p_{pr})p_p^1 + p_{pr}^{'}(1-p_p^1)]$, $d = p_c^1$, and $\pi = (p_1, p_2, p_3, p_4)$.

The transition matrix expression of DH is given by:

$$P = \begin{array}{c} \\ W \\ R \\ N \\ O \end{array} \begin{array}{c} \begin{array}{cccc} W & R & N & O \end{array} \\ \begin{pmatrix} 1-d & d & 0 & 0 \\ 1-ab-c & 0 & ab & c \\ 0 & 0 & ab & 1-ab \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{array} \quad (3)$$

### D. Payoffs

We consider $\alpha$ the level of data disclosure, $\beta$ the probability of the data privacy protection realized by DH (that means $\beta = 1-\alpha$) and $\rho$ the privacy preference of DH. The payoff of DH at each step of the game is defined as: $\pi_h(t) = G - \rho(1-\alpha)t$, where: $t$ is the utility of data record provided by DH, $G$ is the transfer paid to DH, $\alpha$ is the level of data disclosure, $\beta$ is the probability of the data privacy protection realized by DH (that means $\beta = 1-\alpha$ ), and $\rho$ is the privacy preference of DH.

In one game instance, DH's payoff is given by:

Table IV. PROBABILITIES AND CONDITIONS OF DIAGRAM TRANSITIONS.

| Transitions | Conditions | | Probability |
|---|---|---|---|
| **Wait** | | | |
| W1 | Com. Facilities<br>Privacy concession<br>Incentive motiv. | : Favorable<br>: NA (Not App.)<br>: NA | $P(W1) = (1 * p_c^1)$<br>$P(W1) = p_c^1$ |
| W2 | Otherwise | | $P(W3) = 1 - P(W1)$<br>$P(W3) = 1 - p_c^1$ |
| **Request / Response** | | | |
| R1 | Com. Facilities<br>Privacy concession<br>Incentive motiv. | : Favorable<br>: True<br>: True | $P(R1) =$<br>$(1*p_c^1)*[(p_{pr}*p_p^1)+((1-p_{pr}^{'})*(1-p_p^1)]*[p_{inc}*p_i^1+(1-p_{inc}^{'})*p_i^2]$<br>$P(R1) = p_c^1[p_{pr}p_p^1 + (1-p_{pr}^{'})(1-p_p^1)][p_{inc}p_i^1 + (1-p_{inc}^{'})p_i^2]$ |
| R2 | Com. Facilities<br>Privacy concession<br>Incentive motiv. | : Favorable<br>: True<br>: NA | $P(R2) = (1 * p_c^1) * (1 * p_p^1) * [(1-p_{pr}) * p_p^1 + p_{pr}^{'} * (1-p_p^1)]$<br>$P(R2) = p_c^1 p_p^1[(1-p_{pr})p_p^1 + p_{pr}^{'}(1-p_p^1)]$ |
| R3 | otherwise | | $P(R3) = 1 - P(R1) - P(R2)$<br>$P(R3) = 1 - p_c^1[p_{pr}p_p^1 + ((1-p_{pr}^{'})(1-p_p^1)][p_{inc}p_i^1 + (1-p_{inc}^{'})p_i^2] - p_c^1 p_p^1[(1-p_{pr})p_p^1 + p_{pr}^{'}(1-p_p^1)]$ |
| **Negotiate** | | | |
| N1 | Com. Facilities<br>Privacy concession<br>Incentive motiv. | : Favorable<br>: True<br>: True | $P(N1) =$<br>$(1*p_c^1)*[(p_{pr}*p_p^1)+((1-p_{pr}^{'})*(1-p_p^1)]*[p_{inc}*p_i^1+(1-p_{inc}^{'})*p_i^2]$<br>$P(N1) = p_c^1[p_{pr}p_p^1 + (1-p_{pr}^{'})(1-p_p^1)][p_{inc}p_i^1 + (1-p_{inc}^{'})p_i^2]$ |
| N2 | otherwise | | $P(N2) = 1 - P(N1)$<br>$P(N2) = 1 - p_c^1[p_{pr}p_p^1 + (1-p_{pr}^{'})(1-p_p^1)][p_{inc}p_i^1 + (1-p_{inc}^{'})p_i^2]$ |
| **Out of Process** | | | |
| O1 | Com. Facilities<br>Privacy concession<br>Incentive motiv. | : Favorable<br>: NA<br>: NA | $P(O1) = 1$ |

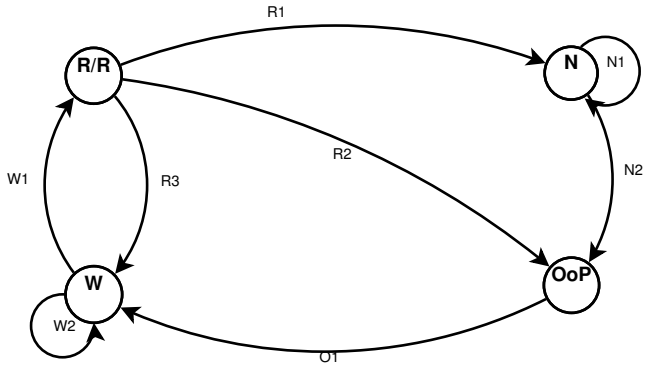


Figure 3. Transitions graph of the game from DH perspective.

$$\pi_{dh}(t) = \begin{cases} G - \rho(1-\alpha)t & \text{if priv. data disclosed} \\ \rho(1-\alpha)t & \text{if priv. data not discl.} \end{cases} \quad (4)$$

The payoff obtained by DR from the trade with one DH is: $\pi_r(t) = I(t) - G$, where $I(t)$ denotes the incentive income. In one game instance, DH payoff is given by:

$$\pi_{dr}(t) = \begin{cases} I(t) - G + \rho(1-\alpha)t & \text{if priv. data disclosed} \\ G - \rho(1-\alpha)t & \text{if priv. data not disclosed} \end{cases} \quad (5)$$

### *E. The Nash equilibrium*

In game theory, every non-trivial game has at least one Nash equilibrium [20]. This equilibrium sometimes requires the use of mixed strategies, rather than pure strategies. In our model, the decision variable of DH is the vector $P_{dv} = (c, i, p)$. As parameter $c$ depends on external factors, adjusting the components of this vector allows controlling the privacy adaptation ($p$) and incentive motivation ($i$), thereby impacting the damage and benefit functions. We consider two sub-functions: a loss function, denoted by $L$, which returns the privacy adaptation, and a gain function $G$, which represents the impact of the incentive motivation on the player's decision.

To express these functions, we choose to use sigmoid representation for the following reasons. It introduces non-linearity in the model which is closer to reality. It has an output between 0 and 1 which may be interpreted as a probability. And, it makes computation easier than arbitrary activation functions. Then, expressions of gain and loss functions are given by:

$$L(p_p) = \frac{1}{1 + e^{-g_p * (p_p - h_p)}} \quad (6)$$

and

$$G(p_i) = 1 - \frac{1}{1 + e^{-g_i * (p_i - h_i)}} \quad (7)$$

Where $p_p$ is probability of adapting privacy, $p_i$ is the probability of adapting the incentive motivation, $g_p$ and $g_i$ are the steepness of sigmoid functions and $g_p$ and $g_i$ are the centers of sigmoid functions. The equilibrium of the game is denoted by $(L*, G*)$ and is found by solving the following optimization problem:

$$max_{P_{dv}}[(1 - L(p_p)).G(p_i)] \quad (8)$$

This type of problems is widely used in economy field to model demand and supply operations. One practical solution is the use of Pareto optimality [21]. The point where the gain and loss curve cross is called the equilibrium point. We already know that privacy adaptation probability $p_p$ depends on user preferences and privacy loss, that means $g_p$ depends on $\rho$ and $\alpha$, as mentioned above. Incentive motivation probability $p_i$ depends on incentive motivation value $I$. For simplicity, and without loss of generality, we will assume that : $g_p = \rho(1-\alpha)$ and $g_i = \sigma I$, where $\sigma$ is an external constant.

## VI. Numerical results

First, we verify Markovian system convergence. Numerically, equation of steady state $\pi = \pi P$ implies:
$p_1 = \frac{1}{1+b+dc+abd+\frac{abd}{a-ab}}$, $p_2 = dp_1$, $p_3 = \frac{abd}{1-ab}p_1$ and $p_4 = (c+ab)dp_1$.

In practice, we use matlab environment to calculate $P^n$ for different values of $n$, as shown in figure 4. Markovian process converges rapidly to the steady state, which is coherent with real situations.

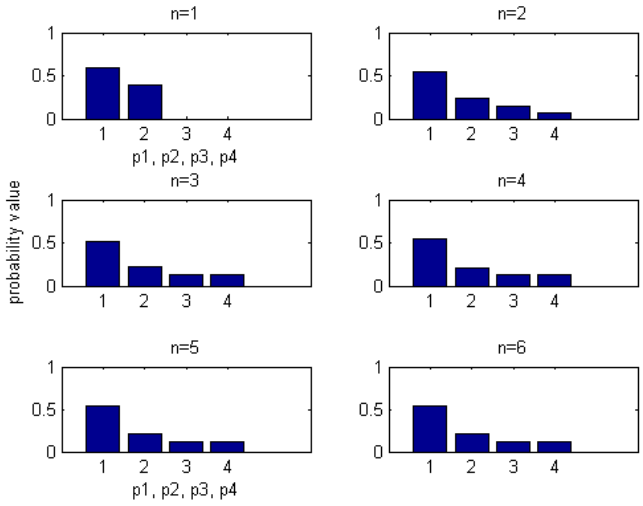


Figure 4. Final states probabilities for different values of n.

Figure 5 shows the variation of damage in function of privacy adaptation requested by DR. We notice that for high value of $p_p$ (DH may likely accept to disclose private data and make concessions), loss increases with privacy concession and decreases with privacy preference severity. The opposite phenomenon occurs for low values of $p_p$.

In figure 6, we show the variation of gain function depending on incentive motivation. For high value of $p_i$ (DH may likely accept to disclose private data for an interesting incentive motivation), gain increases with incentive motivation value.

In figure 7, we use the same gain function (red curve), with fixed incentive value, and variable probability $p_i$. And, we calculate the loss function (blue curve), depending on probability $p_p$. For this function, we chose

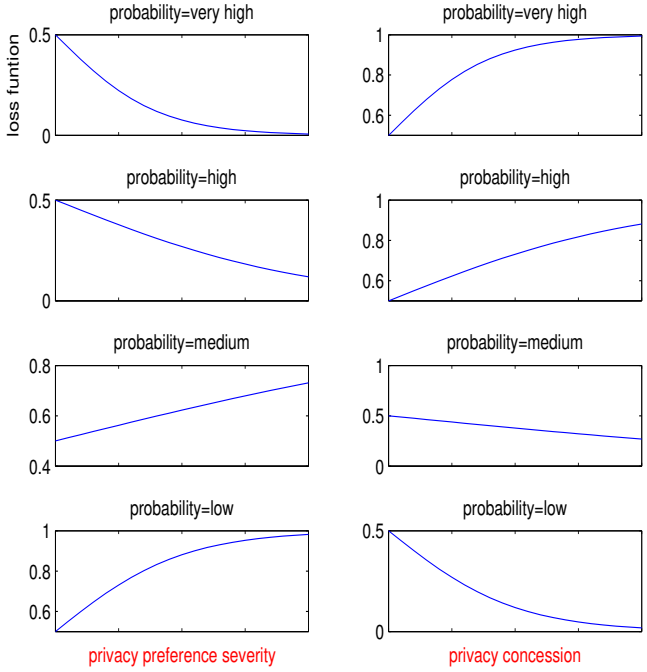


Figure 5. Loss function when the probability of adapting privacy preferences varies.

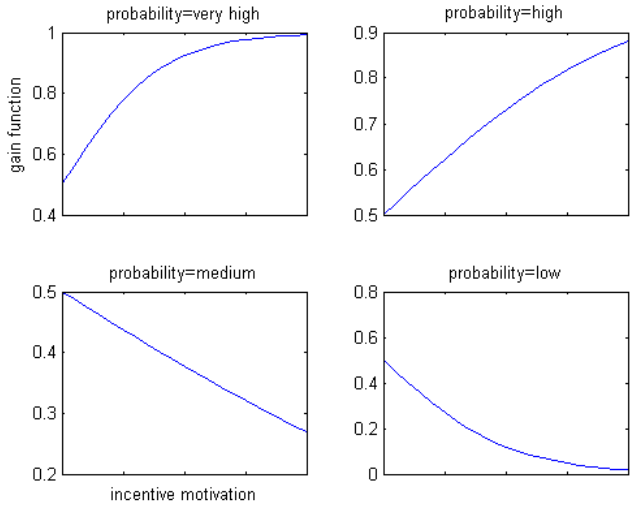


Figure 6. Gain function when the probability of changing the incentive motivation varies.

different levels of privacy severity, that may be fixed by DH (very low -> very high). We deduce that, if DH is severe with his/her data privacy (severity is high), then his/her loss increases, and vice versa. Diagrammatically, we see that the equilibrium point exists and depends on both privacy parameters, and incentive motivation.

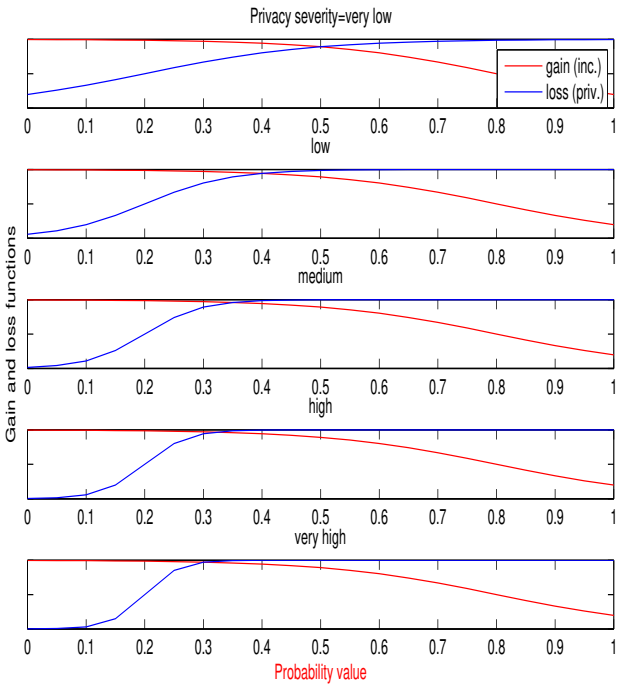


Figure 7. Gain and loss function for fixed incentive and variable privacy severity.

## VII. Conclusion

Our paper contributes in solving open problems related to data privacy in retail applications using game theory. We proposed a Markovian game-based solution to protect private data exchanged when each player aims to maximize his/her payoff. Actors of retail scenarios chose their strategies depending on the potential incentive gain, and privacy loss. By the end of the game (the steady sate of the Markovian process), players reach the equilibrium point with final payoffs. By varying incentive values, and/or privacy preferences, we showed that the equilibrium point position changes. To help players in decision making during the game (actions, transitions and payoffs), all our theoretical findings were validated using numerical results. In the future, we intend to change privacy and incentive parameters and analyze their impact on players behaviors. We will also focus on final players payoffs (after numerous game instances) and their effect on the game strategies.

## References


[1] R. Want, B. N. Schilit, and S. Jenson, "Enabling the internet of things," *Computer*, vol. 48, no. 1, pp. 28–35, 2015.

[2] O. Vermesan and P. Friess, *Internet of Things Applications - From Research and Innovation to Market Deployment*, ser. River Publishers Series in Communications. River Publishers, 2014.

[3] J. Gregory, "The internet of things, revolutionizing the retail industry," Accenture, Tech. Rep., 2015.

[4] T. Kasper, D. Oswald, and C. Paar, *Sweet Dreams and Nightmares: Security in the Internet of Things*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 1–9.

[5] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, pp. 25:1–25:39, Jul. 2013.

[6] E. Jones, "Supermarket pricing and game theory: The presence of walmart," in *American Agricultural Economics Association Annual Meeting*, Colorado, USA, August 2004.

[7] R. R. N. Kanapaka and R. K. Neelisetti, "A stochastic game theoretic model for expanding atm services," *2015 IEEE International Conference on Data Mining Workshop (ICDMW)*, pp. 311–318, 2015.

[8] W. Wang and Q. Zhang, "A stochastic game for privacy preserving context sensing on mobile phone," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, April 2014, pp. 2328–2336.

[9] R. L. Rutledge, A. K. Massey, A. I. Anton, and P. Swire, "Defining the internet of devices: Privacy and security implications," Georgia Institute of Technology, Tech. Rep. GIT-GVU-14-01, 2014.

[10] G. D'Acquisto, J. Domingo-Ferrer, P. Kikiras, V. Torra, Y. de Montjoye, and A. Bourka, "Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics," *CoRR*, vol. abs/1512.06000, 2015.

[11] M. Halkidi and I. Koutsopoulos, "A game theoretic framework for data privacy preservation in recommender systems," in *Proceedings of the 2011 European Conference on Machine Learning and Knowledge Discovery in Databases - Volume Part I*, ser. ECML PKDD'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 629–644.

[12] R. Andres, "Retail and the internet of things: M2m technology building blocks," Eurotech, 2013. [Online]. Available: http://www.eurotech.com

[13] Y. J. Park, "Digital literacy and privacy behavior online," *Communication Research*, vol. 40, no. 2, pp. 215–236, 2013.

[14] A. Viseu, A. Clement, and J. Aspinall, "Situating privacy online: complex perceptions and everyday practices," *Information, Communication & Society*, vol. 7, no. 1, pp. 92–114, 2004.

[15] S. Lace and N. C. Council, *The Glass Consumer: Life in a Surveillance Society*. Policy, 2005.

[16] M. Williams, J. R. C. Nurse, and S. Creese, "The perfect storm: The privacy paradox and the internet-of-things," in *2016 11th International Conference on Availability, Reliability and Security (ARES)*, Aug 2016, pp. 644–652.

[17] M. Olurin, C. Adams, and L. Logrippo, "Platform for privacy preferences (p3p): Current status and future directions." in *PST*. IEEE, 2012, pp. 217–220.

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

[19] Y. Luo, F. Szidarovszky, Y. Al-Nashif, and S. Hariri, "Game theory based network security," *Journal of Information Security*, no. 1, pp. 41–44, 2014.

[20] J. Nash, "Non-cooperative games," *Annals of Mathematics*, vol. 54, no. 2, pp. 286–295, 1951.

[21] H. Aziz, F. Brandt, and P. Harrenstein, "Pareto optimality in coalition formation." in *SAGT*, ser. Lecture Notes in Computer Science, G. Persiano, Ed., vol. 6982. Springer, 2011, pp. 93–104.