ARTICLE IN PRESS

Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

# A game-theoretic model and analysis of data exchange protocols for Internet of Things in clouds

Xiuting Tao [a], Guoqiang Li [a,*], Daniel Sun [b], Hongming Cai [a]

[a] School of Software, Shanghai Jiao Tong University, Shanghai, China

[b] Data61, CSIRO, Australia

## HIGHLIGHTS

- The paper proposes an extensive game based model for behavior analysis of IoT protocols. Analysis techniques are given, with aim to the rationality and fairness properties.
- The properties are proposed to verify the security of business in the cloud computing.
- To verify the properties, a tree analysis method and a linear algorithm are described. As a case study, some flaws of the ASW protocol are identified.

## ARTICLE INFO

*Article history:*
Received 25 May 2016
Received in revised form
20 September 2016
Accepted 22 December 2016
Available online xxxx

*Keywords:*
Exchange protocols
Game theory
Rationality
Fairness

## ABSTRACT

Big data, Internet of things (IoT), and cloud computing have been recognized a family of technologies for a connected world. Besides hailed hope for the future, there are also challenges to security due to complexity and unpredictability of the Internet, clouds, and data. One of the challenges is information and data exchange, for example, identifying untrustworthy cloud users and analyzing abnormal user behavior during information exchange. This paper addresses exchange mechanism, which is a useful theoretic basis to make secure electronic commerce and electronic business transactions possible. To ensure and verify the property of fairness, a crucial property of exchange mechanism, this paper proposes a specific model for behavior analysis based on the extensive game with imperfect information. Rationality and fairness properties are built in the corresponding game and the game tree. To verify the properties, a tree analysis method is proposed, and a linear time algorithm is given. As a case study, some flaws of the ASW protocol are found.



## 1. Introduction

The number of physical objects connected to the Internet is growing at an amazing rate. The Internet of Things (IoT) is a novel paradigm that a variety of things or objects are able to interact with each other and cooperate with their neighbors to reach common goals. There are a lot of domains and environments in which the IoT will play a remarkable role and improve the quality of our lives in the near future, including domotics, transportation, healthcare, and industrial automation [1]. In the IoT, Internet protocols are crucial in the communication of exchange message. For the IoT protocols, security and privacy play a significant role in all markets globally due to the sensitivity of consumers privacy [2].

As the amount of data and information increases, the big data analyzing and informs and supports decision making becomes increasingly important. Big Data analytics is one of the core technologies used by businesses today for decision making and applying game theory data science for strategic decision making, is definitely an intelligent move that will help enterprises predict likely outcomes for businesses, individuals and societies. Games theory is the study of strategic decision making, and games provide alternative means of sharing information and knowledge and participating in decision making. In [3], game theory is applied to model the mechanisms for big data analytics and decision making in the field of geosciences and remote sensing.

Cloud computing is defined as an access model to an on-demand network of shared configurable computing sources such as networks, servers, warehouses, applications, and services. With the rapid development of cloud computing, it brings people to enjoy the convenience such that more lower costs, improved operational efficiency and so on. However more severe information

* Corresponding author.
*E-mail address:* li.g@sjtu.edu.cn (G. Li).

http://dx.doi.org/10.1016/j.future.2016.12.030
0167-739X/

Please cite this article in press as: X. Tao, et al., A game-theoretic model and analysis of data exchange protocols for Internet of Things in clouds, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2016.12.030

security challenges are faced. In the open cloud computing, attackers have a greater temptation, like opening access interface of the cloud, end-users can directly use the cloud and cloud service. For example, Amazon web service does not have any access rights to customer instances and cannot log into the guest operating system; customers may utilize certificate-based SSHv2 to access the virtual instance to share service with others [4]. For the open net work, the middle attack in which the attacker makes independent connections with the victims and relays messages between them, may bring more serious broken than the current use of the Internet to share resources [5]. The behavior of end-user is an important part in the credibility of cloud computing security. Authentication technology is relatively mature, but does not prevent malicious destruction of legal status. The analysis of cloud end-user behavior is a research focus for the cloud computing.

In the open cloud computing, there are some protocol mechanisms and resource allocation mechanisms to exchange and share the electronic resource. Game theory was considered as a formal model for protocol [6–9] and resource allocation [10–14] frequently in recent years. In [15], Chuang Ma had considered an IPv6 control protocol based on game theory to maximize the throughput. J.M. Estevez-Tapiador adopted game theory to model the information of protocols [16]. Chenming Li used a complete information dynamic game model for an automated negotiation protocol [17]. Tian Jun gave a game theory model based on carrier sense multiple access protocol in wireless network [18].

An exchange protocol [19] is fair if at the end of exchange, either each participant receives expected items or neither two receives any useful formation about the other's items. Such protocol example includes *signing of electronic contracts*, *certified e-mail delivery*, and *purchase of network delivered services* [20,21]. Due to difficulties in understanding fairness, there are some definitions given by researchers [22,23].

In [24], the notion of rational exchange is introduced by Syverson in 1998. The rationality is another property of protocol which can replace the fairness to resolve the problem. A rational exchange protocol provides incentives so that rational (self-interested) parties have more reason to follow the protocol faithfully than to deviate from it.

For the rationality and fairness properties, there were some works [25,26,11]. Furthermore, Gu applied game theory and process algebra to analyze the fair exchange protocols [27]. The basic idea of game-based model for fair exchange protocols was offered in [28]. They did not consider the unreliability of network when modeling fairness.

In this paper, an extensive game with imperfect information is adopted to model exchange protocols. The participants are taken as rational players; the communicating messages are actions of players. The rationality and fairness properties are defined on the payoffs of players. An analysis method of the corresponding game tree with its a linear time algorithm is presented to compute weights of leaves on the tree.

The rest of this paper is organized as follows: Section 2 presents some basic concepts of an extensive game in game theory. Section 3 describes how to transform an exchange protocol to an extensive game with perfect information. A formal model of a rational exchange protocol on the subgame perfect equilibrium is presented in Section 4. Section 5 analyzes the Syverson protocol in the model. The relationship with Buttyán's model is shown in Section 6. Sections 7 and 8 consider the fairness property and analyze fair exchange protocol. Section 9 gives the conclusion of this paper.

## 2. Extensive game

This section introduces basic definitions of extensive game theory [29,30] that will be used later.

**Definition 1** (*Extensive Game*)**.** An extensive game with information is a tuple $\Gamma = \langle N, H, P, (\succeq)_{i\in N}\rangle$, where:

- $N$ is a set of players, and $i$ is an element of the set $N$;
- $H$ is a set of action sequences history that satisfies the following three properties:
  1. the empty sequence $\emptyset$ is an element the set $H$,
  2. if $(a^k)_{k=1,\ldots,K} \in H$ (where $K$ may be infinite) and $L < K$, then $(a^k)_{k=1,\ldots,L} \in H$, and
  3. if an infinite action sequence $(a_k)_{k=1}^{\infty}$ satisfies $(a_k)_{k=1,\ldots,I} \in H$ for every positive integer $I$, then $(a_k)_{k=1}^{\infty} \in H$.

  Each member of $H$ is a history, and each component of a history is an action $a \in A$, where $A$ is the action set of players. A history $(a^k)_{k=1,\ldots,K} \in H$ is terminal if it is infinite, or if there is no $a^{K+1}$ such that $(a^k)_{k=1,\ldots,K+1} \in H$. The set of terminal histories is denoted by $Z$.
- $P$ is a player function that assigns to each non-terminal history (the set is denoted by $H\backslash Z$) a member of $N$. In other words, $P(h)_{h\in(H\backslash Z)}$ assigns the player who takes an action after the history $h$.
- $(\succeq)_{i\in N}$ is a preference relation for each player $i \in N$ on $Z$.

The definition of the subgame of the extensive game is given as following,

**Definition 2** (*Subgame*)**.** A subgame of an extensive game $\Gamma = \langle N, H, P, (\succeq)_{i\in N}\rangle$ that follows the history $h$ is an extensive game $\Gamma(h) = \langle N, H|_h, P|_h, (\succeq)_{i\in N}|_h\rangle$, where $H|_h$ is the set of sequences $h'$ of actions for which $(h, h') \in H$. $h' \in H|_h$ for each $\succeq_i|_h$ and $h' \succeq_i|_h h''$ is defined by $(h, h') \succeq_i (h, h'')$, if and only if $h' \in H|_h$.

The extensive game is an explicit description of the sequential structure of the decision problems encountered by the players in a strategic situation. The subgame perfect equilibrium of an extensive game is given as following,

**Definition 3** (*Subgame Perfect Equilibrium*)**.** A subgame perfect equilibrium of an extensive game is a strategy profile $s^*$ such that for every player $i \in N$ and every non-terminal $h \in H\backslash Z$, for which $P(h) = i$, it has

$$O_h(s^*_{-i}|_h, s^*_i|_h) \succeq_i|_h O_h(s^*_{-i}|_h, s_i)$$

for every strategy $s_i$ of player $i$ in the subgame $\Gamma(h)$.

The subgame perfect equilibrium of an extensive game allows the players to find out solutions in which each player can consider his plan of action not only at the beginning of the game, but also at any point of time at which he has to make a decision.

## 3. Exchange protocol game

An exchange protocol is naturally represented as an *extensive game* [29], since during the execution of a given exchange protocol, messages are sent one after one by different participants, until an outcome is reached [25].

A protocol game is considered as follows,

- At each stage, only one of the participants is allowed to perform an action. If there are two or more participants take actions together, this would be modeled as an interleaving of several different stages.
- If someone requires to quit the protocol in others' stage, this requirement is just delayed to his next stage, since other participants only know his quite when he does not perform actions in his stage.

Please cite this article in press as: X. Tao, et al., A game-theoretic model and analysis of data exchange protocols for Internet of Things in clouds, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2016.12.030