SEOULTECH

SeoulTech UCS Lab
Ubiquitous Computing & Security Laboratory

「On Cyber Risk Management of Blockchain Networks : A Game Theoretic Approach (2018)」

Shaohan Feng et al.

Presenter : Lee, Jaedong
(jdlee731@seoultech.ac.kr)

Table of Contents

Introduction

- The risk management and security enhancement to the blockchain users and providers against attacks through the means of the cyber-insurance.

- A few important issues

  (The cyber-insurer's perspective) the scope and policy of the cyber-insurance have to be clearly defined in regard to what kind of attacks to be covered and how to quantify the risk, the possible damage and thus the insurance premium.

  (The reactive risk transfer with the cyber-insurance) rational blockchain providers also have to consider the proactive strategy in security improvement and thus balance the investment in the infrastructure and in the cyber-insurance.

Related Works

Related Works (1/3)

- Permissionless blockchains have been widely recognized for the superb consensus scalability
  - the tamper-evidence data organization and the capability of supporting the distributed, general-purpose virtual machines
- A plethora of emerging application based on blockchains
  - such as Internet finance and property digitization, selforganization for Internet of Things and other nonfinancial applications
- Digitally signed transactions to other nodes by “broadcasting” the transactions in a gossip manner over the P2P links between the nodes
  - The consensus nodes pack up an arbitrary subset of unapproved transactions into a cryptographically protected data structure

Related Works (2/3)

- The honest consensus nodes have to secure a sufficiently large amount of computing power to guarantee the well-being of the blockchain services
- From which the malicious nodes start to breach the blockchain networks
  - Cyber-insurance has been recognized as an innovative tool to manage the cyber risks and alleviate the damage of cyber-attacks for the insured customers
- Cyber-insurance provides the coverage on losses and liabilities from network/information security breaches
  - Compared with classical insurance, cyber-insurance introduces a number of unique issues

Related Works (3/3)

- Nevertheless, recent studies on the mechanisms of doublespending attacks have shed light upon the possible approaches in analytically assessing the risks of this fundamental threat on the blockchain systems
- Based on the characteristics of intentional forking in double-spending attacks
  - it is now possible to estimate the probability of successful double spending and evaluate the potential risks transferred to the cyber-insurers
- Under the condition that the probability distribution of risk can be estimated
  - A risk-adjusted premium for pricing risks based on the Proportional Hazard (PH) transform

System Description and Game Formulation

System Description and Game Formulation

- Preliminaries
  - Successful Attack Probability

$$\mathrm{P}\left(\bar{h}\right) = I_{4(1-\bar{h})\bar{h}}\left(\frac{T}{T_0}\bar{h}, \frac{1}{2}\right), \bar{h} \geq \frac{1}{2}, \tag{1}$$

$$I_w\left(u, v\right) = \frac{\Gamma\left(u+v\right)}{\Gamma\left(u\right)\Gamma\left(v\right)} \int_0^w t^{u-1}(1-t)^{v-1}\mathrm{d}t \tag{2}$$

$$\mathrm{P}\left(\bar{h}\right) = \begin{cases} I_{4(1-\bar{h})\bar{h}}\left(\frac{T}{T_0}\bar{h}, \frac{1}{2}\right), & \bar{h} \geq \frac{1}{2}, \\ 1, & \bar{h} < \frac{1}{2}. \end{cases} \tag{3}$$

System Description and Game Formulation

- System model
  - The User's Utility

$$u_i = \bar{h} + \theta_i - p_i + \alpha \sum_{j \in \mathcal{N}} g_{ij} \Pr\left[\text{j buys the service}\right]. \quad (7)$$

- Profits of the Blockchain Provider and the Cyberinsurer

$$\Pi_{\mathrm{P}}\left(\bar{h}, \mathbf{p}\right) = \sum_{i \in \mathcal{N}} p_i x_i - \frac{a\bar{h}}{1-\bar{h}} + \bar{h}\frac{T}{T_0} N_{\mathrm{T}} r - \underbrace{\frac{T}{T_0} N_{\mathrm{T}} q \int_{1/2}^{1} \left[1 - \int_{1/2}^{t} \mathrm{P}\left(\theta\right) \mathrm{d}\theta\right]^{1/\gamma} \mathrm{d}t}_{\text{premium}}, \quad (8)$$

$$\Pi_{\mathrm{I}}\left(\gamma\right) = \underbrace{\frac{T}{T_0} N_{\mathrm{T}} q \int_{1/2}^{1} \left[1 - \int_{1/2}^{t} \mathrm{P}\left(\theta\right) \mathrm{d}\theta\right]^{1/\gamma} \mathrm{d}t}_{\text{premium}} - \mathrm{P}\left(\bar{h}\right) \bar{h} \frac{T}{T_0} N_{\mathrm{T}} q - \sigma(\bar{h}, \gamma), \quad (9)$$

System Description and Game Formulation

- Profits of the Blockchain Provider and the Cyberinsurer

$$\sigma_1\left(\bar{h}\right)\begin{cases} > 0, & \bar{h} > \frac{1}{2}, \\ = 0, & \bar{h} = \frac{1}{2}, \\ < 0, & \bar{h} < \frac{1}{2}. \end{cases} \tag{10}$$

$$\sigma\left(\bar{h},\gamma\right) = \sigma_1\left(\bar{h}\right)\sigma_2\left(\gamma\right) = \underbrace{\left(\bar{h}-\frac{1}{2}\right)^3}_{\sigma_1(\bar{h})}\underbrace{\left(\gamma-1\right)\gamma^{\beta}}_{\sigma_2(\gamma)}, \quad \beta > 1. \tag{11}$$

Performance Evaluation

Performance Evaluation

- Demonstration of best response and NE

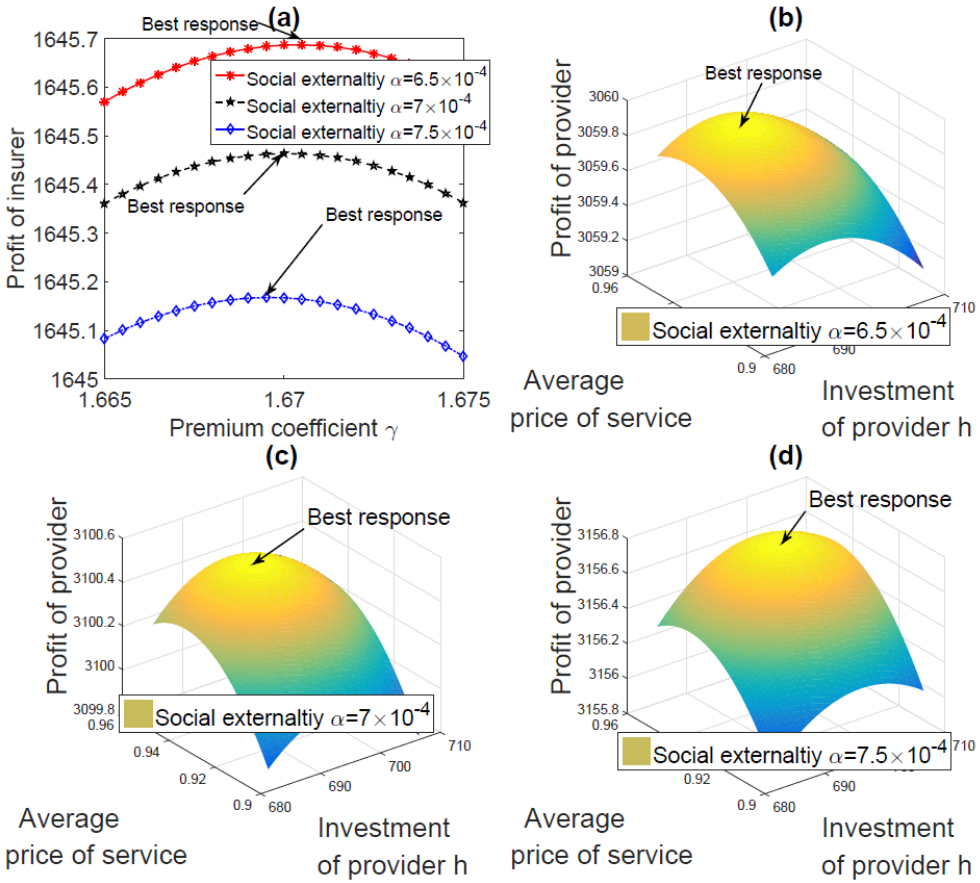

Figure 3: Best response

Performance Evaluation

- Demonstration of best response and NE

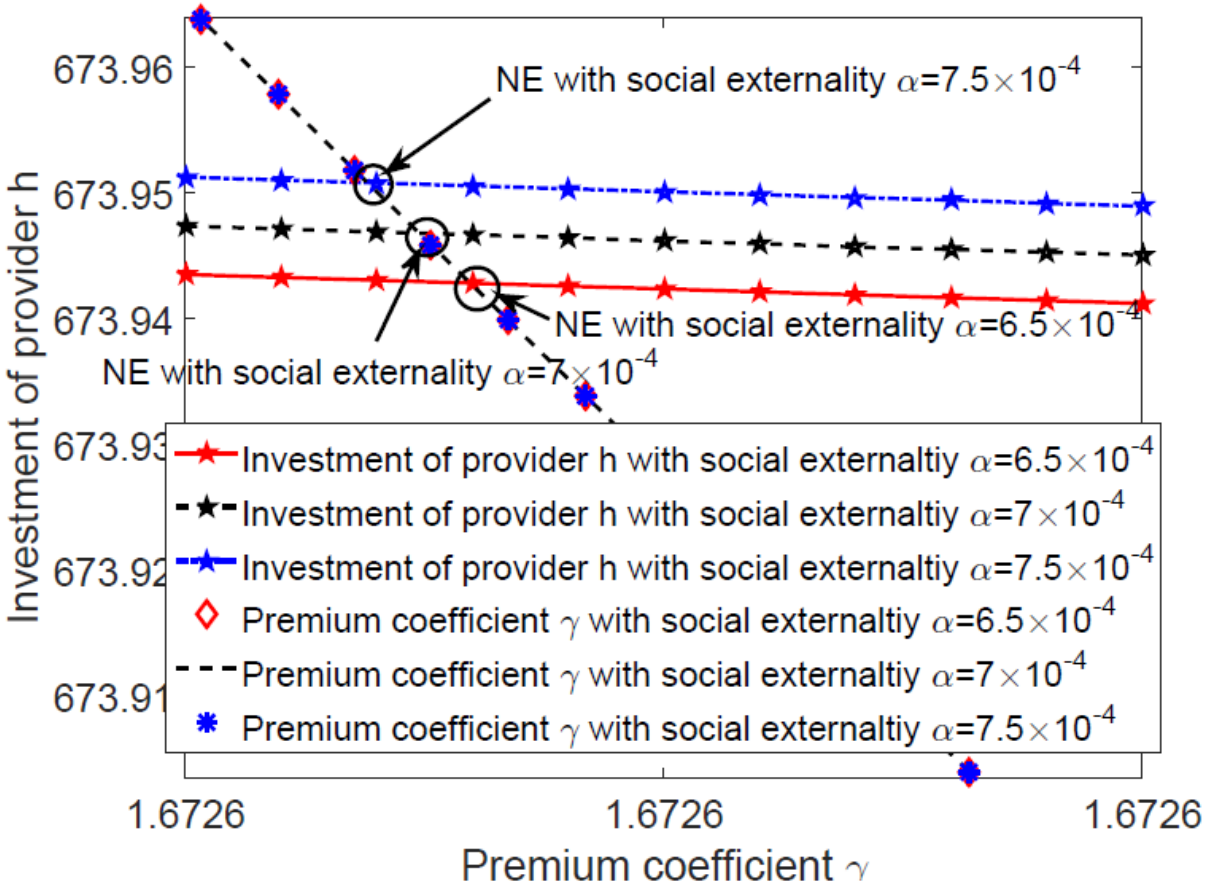

Figure 4: Nash equilibrium

Performance Evaluation

- The impact of the number of users

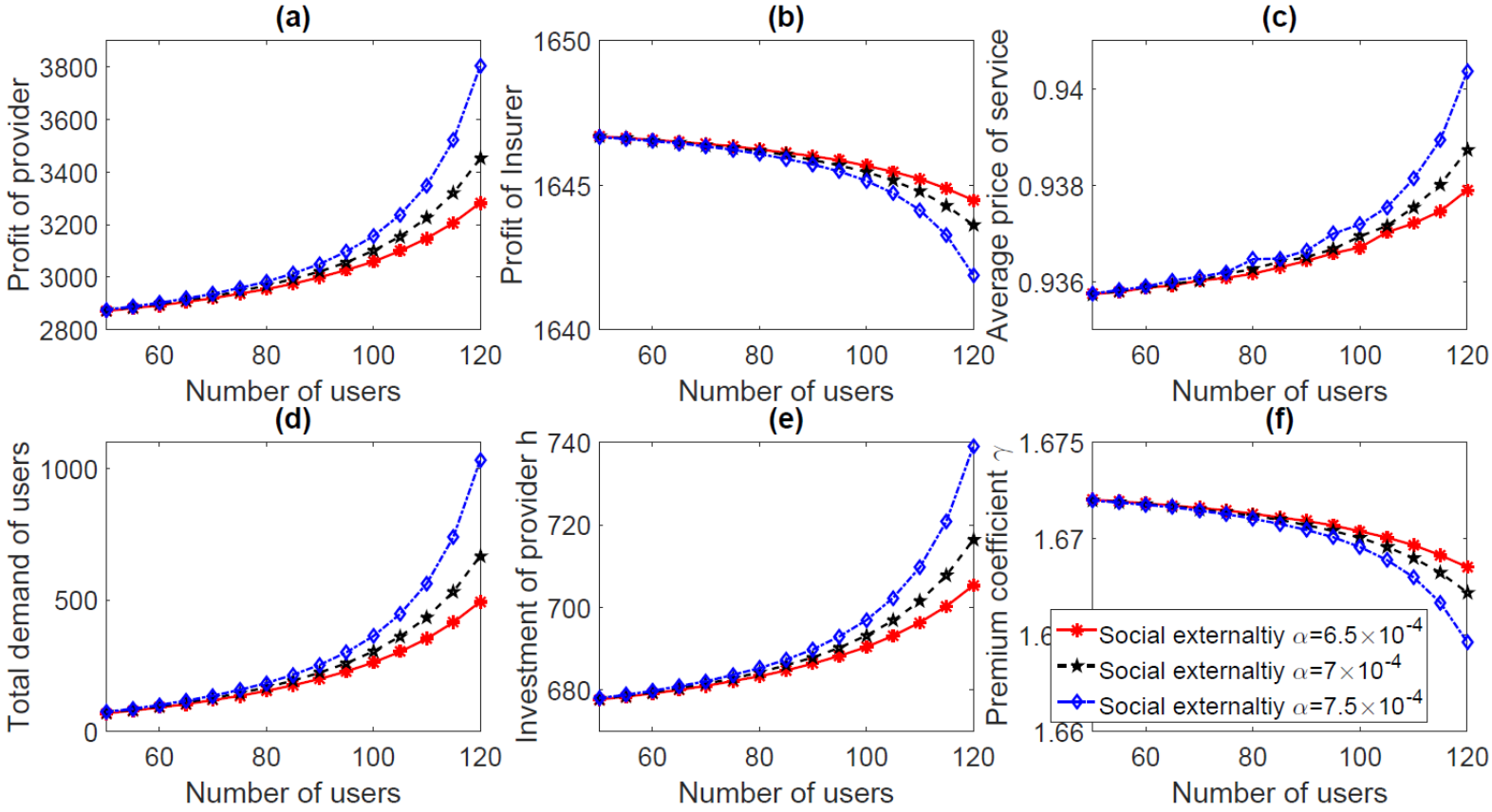

Figure 5: The results with increasing number of users

Performance Evaluation

- The impact of social externality

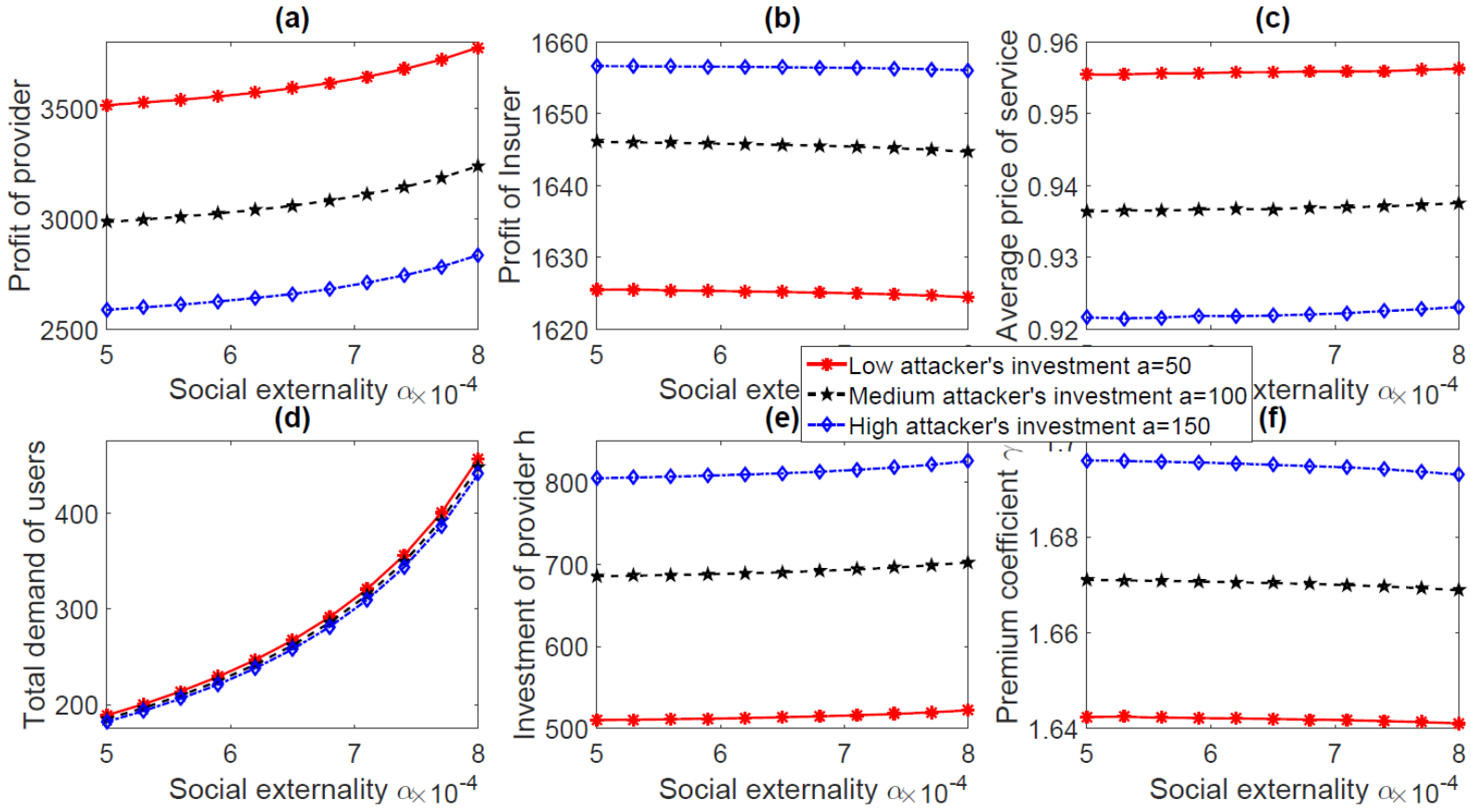

Figure 6: The results with increasing social externality

Performance Evaluation

- The impact of attacker's computing

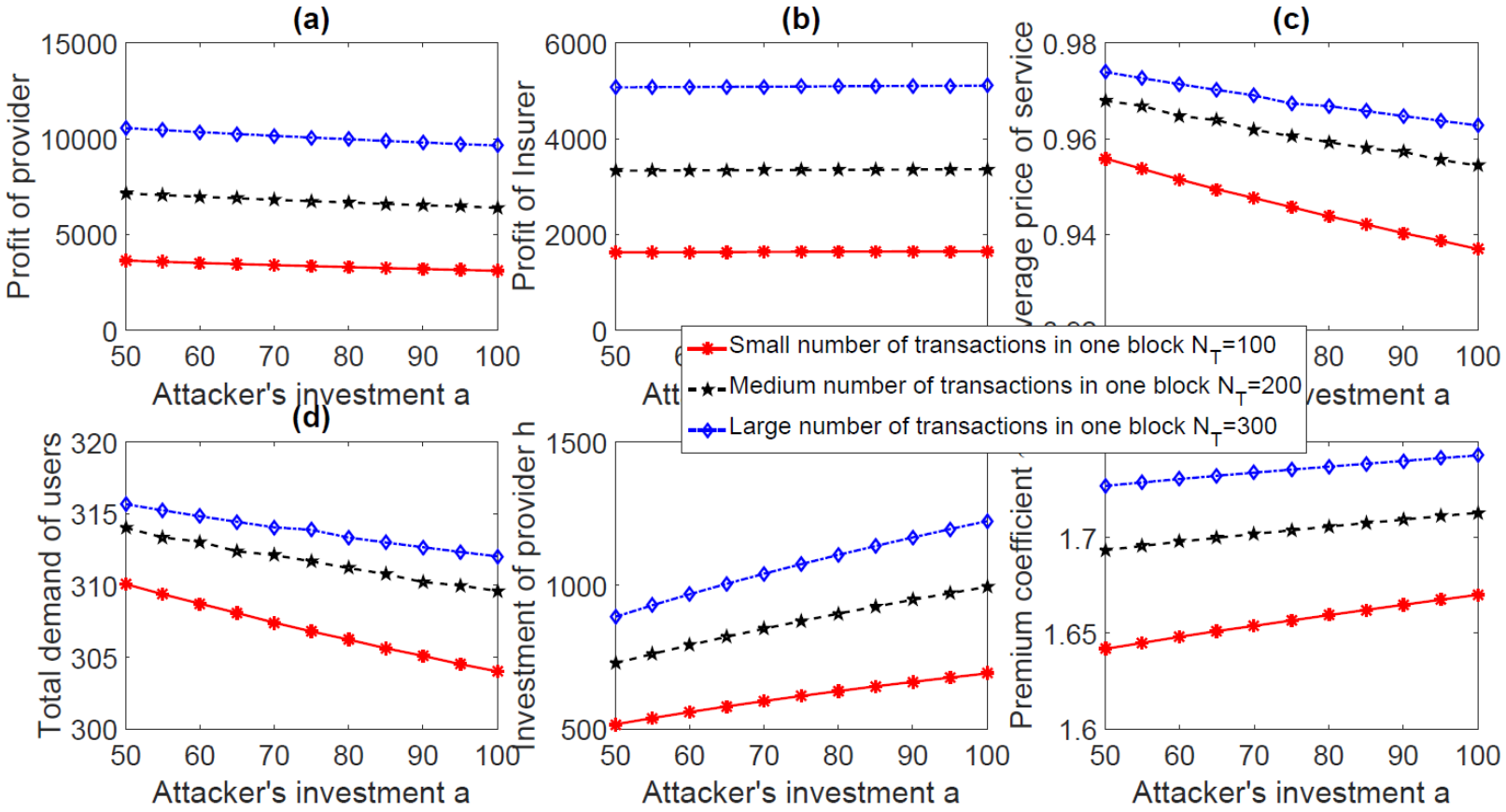

Figure 7: The result with increasing attacker's computing resource

Conclusion

Conclusion

- A risk management framework of the blockchain service market by introducing the cyber-insurance
  - A mean for protecting financially the blockchain provider from double-spending attacks

1. For blockchain provider
   - considered the problem of balancing between the proactive protection strategy
   - investing in computing power
   - the reactive protection strategy purchasing the cyber insurance

2. For the users
   - considered the impact of both the social externality
   - the service security on the users' valuation of the blockchain service

3. For the cyber-insurer
   - incorporated the risk adjusted pricing mechanism for premium adaptation