Reliability Engineering and System Safety 99 (2012) 45–54

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

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

A game theoretic framework for evaluation of the impacts of hackers diversity on security measures

Behzad Zare Moayedi, Mohammad Abdollahi Azgomi *

School of Computer Engineering, Iran University of Science and Technology, Hengam Street, Resalat Square, Tehran 16846-13114, Iran

ARTICLE INFO

Article history:
Received 19 November 2010
Received in revised form
31 October 2011
Accepted 3 November 2011
Available online 10 November 2011

Keywords:
Security
Modelling
Quantitative security evaluation
Markov chains
Game theory

ABSTRACT

Game theoretical methods offer new insights into quantitative evaluation of dependability and security. Currently, there is a wide range of useful game theoretic approaches to model the behaviour of intelligent agents. However, it is necessary to revise these approaches if there is a community of hackers with significant diversity in their behaviours. In this paper, we introduce a novel approach to extend the basic ideas of applying game theory in stochastic modelling. The proposed method classifies the community of hackers based on two main criteria used widely in hacker classifications, which are motivation and skill. We use Markov chains to model the system and compute the transition rates between the states based on the preferences and the skill distributions of hacker classes. The resulting Markov chains can be solved to obtain the desired security measures. We also present the results of an illustrative example using the proposed approach, which examines the relation between the attributes of the community of hackers and the security measures.

1. Introduction

With significant growth in the complexity of information systems, it is necessary to have automatic methods for evaluation of the security of these systems. The required methods should be powerful enough to support the variations of the systems and to introduce quantitative measures of their security states. Although, there have been significant advances in this way, it is true to say that until now, there has not been a complete response to the problem of quantitative security evaluation. The main reason is the inherent difficulties of modelling the intentional human-made security-related events. Usually, attack process and its consequences in an information system is highly affected by decisions of human agents, whether hackers or the defending mechanisms of the systems [1–5]. During an attack process, a hacker chooses an action among a set of different possible actions at each internal step of the process. Likewise, the system administrator may arrange some plans to thwart the attack. Each decision made by these two opponents follows a rich set of properties of its performer such as: motivation, skills, possibilities and the current amount of knowledge about the system. Until now, these complexities have prevented the efforts to succeed in creation of efficient and comprehensive methods for modelling and precise evaluation of human agent behaviours.

In the existing methods of human behaviour modelling, some of the game theoretical methods are preferred over the others due to their realistic considerations of the rationality of agents. As an example, in [6], Cavusoglu and Raghunathan have compared decision theory and game theoretic approaches to the problem of decision theory against strategic fraudsters. They have concluded that game theory is preferable over decision theory except in case of simultaneous-move game where the configuration parameters of decision theory and game theory are sufficiently close. They have also compared the limitations of these two approaches.

The game theoretical models have already been used in dependability analysis. However, until recent years, it was not applied to security analysis. In the past few years, some game theoretical models have been developed for examining the effects of strategic interactions in system dependability. These models provide initial methods to optimise system dependability against intelligent threats. The existing approaches have evolved from simple one-period game models to complicated models for repetitive strategic interactions. In the area of quantitative evaluation of security the new trend is to use game theory in dependability modelling of sophisticated systems in order to consider intentional events and to propose optimal defensive resource allocations [7–9].

One of the most straightforward applications of game theory in dependability analysis is based on the idea of augmenting

* Corresponding author. Fax: +98 21 77240469.
E-mail addresses: behzad_moayedi@comp.iust.ac.ir (B. Zare Moayedi), azgomi@iust.ac.ir (M.A. Azgomi).

0951-8320/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2011.11.001

stochastic modelling by game theoretical opponents' behaviour predictions [10]. This approach incorporates the malicious failures in the normal process of dependability evaluation by making a correspondence between the stochastic model of the system and a game model of the strategic interactions of the system and the hackers. There will be a stochastic model like a Markov chain model and a corresponding stochastic game model with the same specification of the state space. Both models use the same set of system states. The final transition rates between the states are computed based on the normal stochastic rates of accidental failures and the solution of the game model representing the malicious failure rates.

This method offers new insights into dependability analysis, especially because of its clear resolution between the problem of human behaviour prediction and the main problem of stochastic modelling. However, it has some limitations that arise from the basic challenges of game theory [7]. The incomplete knowledge of players about the game rules, the other players' possibilities and the overall game are examples of these challenges. These limitations will challenge any game theoretic approach for dependability analysis. However, in the approach proposed in this paper, we have dealt with some marginal limitations of this method, which are not directly related to the basic challenges of game theory.

Usually, computer systems are exposed to attacks from a large number of hackers with diverse behaviours. Despite this fact, almost all existing game theoretic approaches in the field of quantitative evaluation of security concentrate on a limited number of hackers and defensive mechanisms of systems. They do not consider the large number of hackers and the diversity in their behaviours. The main challenge of game theoretic approaches in this situation is the explosion of the sate space. The size of the state space grows exponentially, due to growth in the number of players (i.e. hackers and defenders). If there is a large set of hackers, the game model cannot be solved easily.

In [8,10,17–20], game theory in combination with continuous-time Markov chains (CTMCs) has been used for modelling attacker behaviour. Our aim has been to extend this work [21,22]. In this paper, we introduce a game theoretic approach for quantitative evaluation of security measures by considering hackers (and defenders) with diverse behaviours. We propose a novel approach to extend the basic ideas of using game theory for predicting the transition rates in stochastic models. The proposed method classifies the community of hackers based on two main criteria widely used in hacker classifications, which are motivation and skill. The former classifies the community of hackers into different classes with different behaviour and objectives. The latter provides a method to calculate the effects of each hacker's efforts in the results of the game model. The proposed method is logically straight and the results are satisfactory. We have used CTMCs to model the system. Based on the preferences of each class of hackers and the distribution of skills in each class, the transition rates between the states are computed. The resulting CTMC can be solved to obtain the desired security measures of the system. Because, the problem of state space explosion is most likely to happen in attacker–defender models when there are significant diversity and multiplicity, the proposed method addresses this problem in a reasonable manner, which makes the approach more flexible and usable.

The rest of this paper is organised as follows. In Section 2, some related works are surveyed. In Section 3, some motivations of this work are mentioned. In Section 4, the problem is formulated. In Section 5, the proposed approach is presented. In Section 6, an illustrative example is given. In Section 7, some important aspects of the proposed method are discussed. Finally, some concluding remarks are mentioned in Section 8.

2. Related work

Early efforts for using game theory in dependability analysis have focused on relating the probabilistic risk analysis models to basic game theory models in order to incorporate the effects of strategic interactions on the dependability of systems. For example, in [11], a model has been introduced to address the economical issue of resource assignment for information security risk mitigation. The model tries to figure out the optimal point of investment due to the system vulnerability assessment and shows that for a given potential loss, a firm should not necessarily focus its investments on information sets with the highest vulnerability. Rather, it suggests that to maximise the expected benefit from investment to protect information, a firm should spend only a small fraction of the expected loss due to a security breach.

In [12], a general model has been proposed that considers the system dependability as a general tool and merges game theory with system dependability analysis. This work is very important, because it has shown the first organised relation between the dependability analysis and game theory and utilises the system dependability as a general tool.

In [1], a probabilistic risk analysis method is proposed, which focuses on the case in which different players assess the system reliability differently and conflict arises in resource allocation decisions. In this method, each component of the system is modelled as an individual player and the reliability of each component, depends on the component's strategies and technical characteristics.

In [13], a model has been introduced that connects the probabilistic risk analysis, the Bayesian influence diagram and game theory for analysis of terrorist risks. While the model has not focused on dependability analysis of systems, the results are useful for this purpose.

One of the first researches on applying game theory in dependability analysis that directly addressed the defensive resource allocation was conducted by Bier et al. [14], which was based on [1]. They have focused on a more accurate dependability model. As reported in [15], they have continued their work based on the following assumptions: (1) the hacker acts rationally to maximise the predictable damages of attacks, (2) the attacks in different parts of the system, either successful or unsuccessful, are independent and (3) the failure time is not important. The result shows that the system failure probability increases as the hacker's knowledge about the defensive mechanisms grows.

In [16], a game theoretical model is introduced for resource allocation in serial, parallel or more general systems. In this model, it is assumed that the defender's aim is to maximise the cost of attack for hackers as much as possible. In addition, it is assumed that by increasing the defensive measures in each part of the system, the cost of attack will increase, but the probability of a successful attack will not necessarily decrease. This assumption is a logical drawback in the attack preventing problems, especially when the hacker encounters the shortage of resources. In these situations, increasing the cost of attack may lead to cost overruns of available resources for hackers.

In [9], Nguyen et al. have studied a stochastic game theoretic approach to security. They have modelled the interactions between hacker and system, as a two player stochastic game and with a network, whose nodes indicate the assets of system and their vulnerabilities; they have formulated the complex dynamics of system under the processes of attacks.

In [8,17–20], Sallhammar et al. have proposed a sound framework for integrated dependability and security evaluation. In traditional dependability, the origin of errors is accident and intentional errors are neglected. Although, this framework is