Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Analysis on the acceptance of Global Trust Management for unwanted traffic control based on game theory

Yue Shen [a], *Zheng Yan* [a,b,*], *Raimo Kantola* [a]

[a] *Department of Communications and Networking, Aalto University, Espoo, Finland*
[b] *The State Key Lab of ISN, Xidian University, Xi'an 710071, China*

ARTICLE INFO

Article history:
Received 17 December 2013
Received in revised form
19 March 2014
Accepted 22 March 2014
Available online 5 April 2014

Keywords:
Game theory
Social dilemma
Public goods game
Trust management
Unwanted traffic control
Equilibrium

ABSTRACT

The Internet has witnessed an incredible growth in its pervasive use and brought unprecedented convenience to its users. However, an increasing amount of unwanted traffic, such as spam and malware, severely burdens both users and Internet service providers (ISPs), which arouses wide public concern. A Global Trust Management (GTM) system was proposed and demonstrated to be accurate, robust and effective on unwanted traffic control in our previous work (Yan et al., 2011, 2013). But its acceptance by network entities (ISPs and hosts) is crucial to its practical deployment and final success. In this paper, we investigate the acceptance conditions of the GTM system using game theory. Considering the selfish nature of network entities, we address our problem as a social dilemma. To enhance cooperation among network entities, a public-goods-based GTM game is formulated with a trust-based punishment mechanism that can provide the incentives of behaving cooperatively for network entities. Meanwhile, the conditions of the adoption of GTM system are figured out. We also carry out a number of simulations to illustrate the acceptance conditions of the GTM system in practical deployment, and show the effectiveness of the trust-based punishment mechanism. Furthermore, suggestions for ISPs cooperating with antivirus vendors are put forward.

1. Introduction

The Internet has witnessed an incredible growth in its pervasive use. People are enjoying unprecedented convenience brought by the Internet boom. However, at the same time when Internet users benefit from the Internet, they are more and more troubled by the increasing amount of unwanted traffic, such as spam, malware, vicious intrusions, and so on. For example, spam accounts for 14.5 billion messages globally per day, i.e., it makes up 45% of all emails (http://www.symantec.com/about/news/release/article.jsp?prid=20120429_01). According to South Korea's National Police Agency, the computer networks of three major South Korea banks and three television networks went offline almost at the same time on 20th March 2013, caused by a

* Corresponding author. State Key Lab of ISN, Xidian University, Xi'an 710071, China.
E-mail addresses: yue.shen@aalto.fi (Y. Shen), zheng.yan@aalto.fi, zhengyan.pz@gmail.com, zyan@xidian.edu.cn (Z. Yan), raimo.kantola@aalto.fi (R. Kantola).

http://dx.doi.org/10.1016/j.cose.2014.03.010
0167-4048/

malware attack (forum.isvoc.com/43172.htm). The websites and corporate networks at Bank of America, JPMorgan Chase and Citigroup suffered from distributed denial-of-service (DDoS) attacks both in 2011 and 2012, resulting in hundreds of complaints from their customers (www.nbcnews.com/technolog, 1260). Such incidents undoubtedly increase public worries on network security. Thus, working out an efficient solution to control the unwanted traffic in the Internet has become a crucial task that brooks no delay.

To deal with unwanted traffic, technologies like firewalls, network monitoring, and intrusion detection systems (IDS) are widely used, achieving certain positive effects. Quite a number of approaches have been put forward for controlling spam, malware, and DDoS attacks (Zheleva et al., 2008; Vasudevan, 2008; Choi et al., 2010). In our previous work, we proposed a Global Trust Management (GTM) system, which executes accurate, effective and robust unwanted traffic control based on trust evaluation on each network entity (Yan et al., 2011, 2013). But in real practice, whether network entities (e.g., ISPs and their subscribed hosts) have willingness to accept and adopt such a system greatly affects the success of system deployment. There exists a social dilemma that a cost suffered by cooperative entities that adopt GTM would generate a benefit shared by all, so entities involved would prefer to take a free ride (i.e., not adopt GTM) as long as their utilities could be maximized. But this selfish behavior will make everyone worse off and finally degrade the performance of the GTM system.

In this paper, we apply game theory to analyze the acceptance of the GTM system for unwanted traffic control. We respectively analyze the social dilemma in both host layer and ISP layer. A public goods based GTM game is formulated, considering the quality of network environment as public goods. In each layer, we explicitly compare entities' utilities for taking adverse (cooperative/uncooperative) strategies and find out the system weakness. Next, we introduce a trust-based punishment mechanism in order to stimulate network entities to accept and adopt the GTM system by contributing to the system. That is, whether an entity should get punishment depends on its trust value, which is directly related to its contribution to the system. We further put forward suggestions for ISPs on operating strategies to cooperate with antivirus vendors to achieve a win–win situation. Specifically, the contributions of our paper are described as below:

1) This paper is one of the first to address the problem of network entities' cooperation on unwanted traffic control as a social dilemma.
2) We formulate a mechanism to arouse the network entities' willingness to contribute to the GTM system and analyze it by applying game theory;
3) We analyze the acceptance and adoption conditions for the GTM system.
4) We conduct a number of simulations to illustrate the acceptance conditions of the GTM system in practical deployment, and show the effectiveness of the trust-based punishment mechanism.

The rest of the paper is organized as follows. Background and related work section gives a brief review of the game theory, social dilemma and related work. System model section describes our system model and research assumptions. Public-goods-based GTM game is formulated to analyze the social dilemma and a trust-based punishment mechanism is proposed to mitigate the dilemma in Public-goods-based GTM game section, followed by simulation and evaluation results in Evaluation: simulation results and analysis section. The suggestion on ISPs' operating strategies is given in Further discussions section. Finally, conclusion is summarized in the last section.

2. Background and related work

2.1. *Game theory*

Game theory is the study of mathematical models of conflict and cooperation between intelligent rational decision-makers (Myerson, 1991). A rational player tries to take strategic actions in iterations to produce (mostly to maximize) a utility it desires, and the utility is the difference between benefit and cost. Game theory has a wide range of usage in economics, political science, biology, and so on. Nowadays, it has come to play an increasingly important role in modeling and analyzing competing behaviors of interacting parties over the Internet. For example, to encourage workers' contributions to "crowdsourcing" website, a two-sided market model was formulated and gift-giving games were played repeatedly between requesters and workers, based on which a novel class of incentive protocols was proposed and proved to make the website operation close to Pareto efficiency (Zhang and Van der Schaar, 2012). A selfish behavior in collaborative groups of social applications was modeled and its impact was studied using a repeated game in (Al-Dhanhani et al., 2012). However, simulation results show that Tit-for-Tat strategies cannot solve the problem (selfish behavior) and the features that can motivate selfish users to become cooperative are needed in social applications. Papaioannou and Stamoulis studied the submission of dishonest ratings in electronic markets (Papaioannou and Stamoulis, 2008). They first conducted a single-shot game, proving that under certain initial system conditions, honest feedback can be a stable equilibrium for the whole market. Then, the game model was refined for repeated transactions and reputation-based fines were implemented, which enabled the submission of honest feedbacks as a stable Nash equilibrium of the game. In game theory, a set of strategies is a Nash equilibrium if no player could be better off by unilaterally changing her current strategy. That is, no player has an incentive to change her action (http://www.gametheory.net/dictionary/NashEquilibrium.html).

2.2. *Social dilemma*

Social dilemmas are situations faced by a group of individuals where short-term self-interests are at odds with long-term group interests, so that the individuals have to choose whether to cooperate for the good of the group or to defect for personal gain bearing in mind that the whole group finally suffers if everyone defects (Greenwood, 2010). Social dilemmas