Computer Networks 74 (2014) 103–113

Contents lists available at ScienceDirect

Computer Networks

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

Containing smartphone worm propagation with an influence maximization algorithm

Sancheng Peng [a,b], Min Wu [a], Guojun Wang [a,*], Shui Yu [c]

[a] School of Information Science and Engineering, Central South University, Changsha 410083, China
[b] School of Computer Science, Zhaoqing University, Zhaoqing 526061, China
[c] School of Information Technology, Deakin University, 221 Burwood HWY, Burwood, VIC 3125, Australia

ARTICLE INFO

Article history:
Received 26 December 2013
Received in revised form 1 September 2014
Accepted 1 September 2014
Available online 22 September 2014

Keywords:
Smartphones
Worm containment
Influence maximization
Social relationship graph
Voting algorithm
Immunization

ABSTRACT

In recent years, wide attention has been drawn to the problem of containing worm propagation in smartphones. Unlike existing containment models for worm propagation, we study how to prevent worm propagation through the immunization of key nodes (e.g., the top k influential nodes). Thus, we propose a novel containment model based on an influence maximization algorithm. In this model, we introduce a social relation graph to evaluate the influence of nodes and an election mechanism to find the most influential nodes. Finally, this model provides a targeted immunization strategy to disable worm propagation by immunizing the top k influential nodes. The experimental results show that the model not only finds the most influential top k nodes quickly, but also effectively restrains and controls worm propagation.

1. Introduction

The number of smartphones in use is steadily increasing, as they are becoming more and more popular. For an increasing percentage of users, smartphones have become an integral part of their everyday lives. Moreover, all smartphones are now being equipped with advanced features, such as SMS (short messaging services), and MMS (multimedia messaging service) [1,2]. SMS and MMS attract more and more people due to their convenience, speed, and economic characteristics, making them a common means of communication in the daily lives of people. However, the significant development and pervasive use of smartphones also has attracted worm writers to pursue their malicious goals by exploiting smartphones' vulnerabilities [3].

According to recent security reports [4–8], the number of malicious exploits and executed attacks has recently surged. In 2010, more than 1 million cell phone users in China were infected by the 'Zombie' virus, which can automatically send text messages, and the attack resulted in a loss of $300,000 per day. The Juniper Networks Mobile Threat Center (MTC) released its *2011 Mobile Threats Report* in February 2012, which reported that mobile malware increased 155% across all platforms over the previous year, and provided evidence of a new level of maturity in the security threats aimed at mobile devices.

The *influence* of a node reflects its importance in a social network. The reason is that a node with a larger influence usually has more connections with others. Therefore, it is extremely important for us to design an effective and efficient mechanism to find the top k influential individuals, something which remains an important yet challenging problem [9]. Most of the existing models focus on greedy algorithms and mainly suffer

* Corresponding author.
E-mail addresses: min@csu.edu.cn (M. Wu), csgjwang@csu.edu.cn (G. Wang).

http://dx.doi.org/10.1016/j.comnet.2014.09.004
1389-1286/

from low computational efficiency, greatly hindering their application to real-world social networks. Although the existing models provide some valuable insights into the problem of influence maximization in social networks, strategies based on greedy algorithms fail to decrease the complexity.

Due to the scale-free characteristics of mobile social networks, a traditional immunization strategy [10], such as a random immunization strategy, a targeted immunization strategy, or an acquaintance immunization strategy, remains a huge challenge: a random immunization strategy needs to immunize 80 percent of the total number of nodes, a targeted immunization strategy requires knowing the global topology of the network, and an acquaintance immunization strategy needs to vaccinate the highly-connected important nodes.

How can we find the important nodes quickly and contain worm dissemination by immunizing these nodes? To answer this question, we need to evaluate which nodes are important without prior knowledge of the global network topology, and decrease the computational complexity for finding the important nodes in large-scale networks. In this paper, we present a novel approach that can significantly reduce the running time, can identify the most influential k nodes effectively and accurately without information about the global topology of the network, and effectively control worm propagation in a network. The contributions of our work are summarized as follows:

- We establish a social relationship graph based on the theory of complex networks. This graph is constructed using the actual SMS/MMS communication data from people's daily lives for social interactions. It is built to reveal the connections of social interaction and the spreading of SMS/MMS.
- We design a method of analysis of the behavior of a mobile social network based on the social relationship graph. The related factors of behavior analysis and their computing model are provided in this method, and they are used to count and analyze the characteristics of the mobile social network, such as in-degree, out-degree, the number of friends, activity degree, and intimacy degree.
- We design a mechanism to mine the top k influential nodes based on a voting algorithm. In this mechanism, each node for votes the most influential node among its set of friend nodes, according to the intimacy degree with these friends. Then, the heap sorting algorithm is employed to sort the results of the voting to discover the most influential former k nodes.
- We find that the immunization of the top k influential nodes can disable worm propagation more effectively than the traditional random immunization strategy or acquaintance immunization strategy, based on the worm propagation model presented in [1,2], and by improving the targeted immunization strategy.
- Extensive simulations using a real-world SMS/MMS-based communication data set demonstrate that the proposed algorithm is more effective and efficient than the existing models.

The remainder of this paper is structured as follows: In Section 2, we provide an overview of related work. We discuss the construction of the social relationship graph in Section 3. In Section 4, we perform an analysis seeking the factors of node influence and their computing models and present a mechanism to mine the influential top k nodes in Section 5. In Section 6, we design a containment scheme and provide the results of a model validation in Section 7. Finally, we conclude this paper in Section 8.

2. Related work

In this section, we review related work in terms of three dimensions. The first dimension is the worm propagation modeling; the second is related to the influence maximization algorithm; and the last one is related to worm containment models.

2.1. Worm propagation modeling

Zheng et al. [11] focused on modeling population distribution density, Bluetooth radius, and node velocity. They pointed out a variety of quarantine methods that could greatly reduce the potential poisoning. But the authors did not consider the impact of individual differences on the propagation dynamics of different worms, and did not characterize the effect of the real-world social interactions on the propagation dynamics of Bluetooth worms.

Yan and Eidenbenz [12] presented a model to study the spread of Bluetooth worms and investigated the impact of mobility patterns on Bluetooth worm propagation. In their proposed model, the impact of mobility patterns on Bluetooth worm propagation can be investigated by introducing some input parameters, such as the average node degree, average node meeting rate, and the link duration distribution. However, it is difficult to apply this model to analyze the propagation of SMS/MMS worms.

Peng and Wang [13] proposed a worm propagation modeling scheme (WPM) that used two-dimensional (2D) cellular automata to simulate the dynamics of the worm propagation process from a single node to the entire Bluetooth network. Although the WPM scheme integrates an infection factor and a resistance factor, it fails to provide specific expressions to compute these two factors.

Ruitenbeek et al. [14] proposed response mechanisms to analyze the effects of multimedia messaging system (MMS) viruses that spread by sending infected messages to other phones. Fleizach et al. [15] developed an event-based simulator to evaluate the effects of malware propagation using communication services like VOIP and MMS in mobile phone networks. However, they did not use real traffic data in their worm propagation model.

Peng et al. [16] proposed an approach to characterize the propagation dynamics of SMS/MMS-based worms. The authors introduced social network theory to characterize mobile worms that spread using MMS or SMS and typically exploit the social network of users to propagate from one mobile device to another. Moreover, the impact on the malware propagation of individual differences was also taken into account.