Simulation Modelling Practice and Theory 50 (2015) 176–188

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

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

On monitoring and predicting mobile network traffic abnormality

Yingxu Lai [a,*], Yinong Chen [b], Zenghui Liu [c], Zhen Yang [a], Xiulong Li [a]

[a] College of Computer Science, Beijing University of Technology, Beijing 100124, China
[b] School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tempe 85287, USA
[c] Automation Engineering Institute, Beijing Polytechnic, Beijing 100176, China

ARTICLE INFO

Article history:
Available online 4 March 2014

Keywords:
Network attack
Traffic behavior
Traffic monitoring
Feature set
Feature selection

ABSTRACT

Traffic analysis and traffic abnormality detection are emerged as an efficient way of detecting network attacks in recent years. The existing approaches can be improved by introducing a new model and a new analysis method of network user's traffic behaviors. The description dimensions to network user's traffic behaviors in the current approaches are high, resulting in high processing complexity, high delay in differentiating an individual user's abnormal traffic behavior from massive network data, and low detection rate. To improve the detection rate and efficiency, we develop a new method of establishing user's traffic behavior analysis system based on a new model of network traffic monitoring. First, we establish a more complete feature set based on the characteristics of network traffic to describe massive network user's behaviors. Then, we define a feature selection rule based on the relative deviation distance to select the optimized feature set. We use the selected feature set to locate the abnormality moment and the users who produce the abnormal traffic behavior. Finally, a traffic behavior analysis method based on prediction is developed to improve efficiency of the system. This new method is applied to evaluate the mobile users on mobile cloud. The experimental results show that the proposed method has a higher detection rate and lower delay in the analysis of abnormal user's traffic behavior than that of the existing approaches.

1. Introduction

With the explosive development of mobile applications and the support of Cloud Computing (CC) for a variety of services for mobile users, Mobile Cloud Computing (MCC) [1] is introduced as an integration of CC into the mobile environment. MCC is a model developed as a solution to overcome the challenges in mobile devices using CC services like storage and computing resources [2,3]. Experience with Internet-based services has shown that attacks from worms and viruses such as Code Red and SQL Slammer are common threats to network-oriented applications. Threats also exist in mobile devices, cloud side, and the communication channels, through attacks such as packet injection and Man-in-the-Middle. Mobile devices can access MCC in many different ways, including voice service, Short Messaging Service (SMS) and other Internet service through phone networks. In addition, most smart phones can also access to the network through Wi-Fi and Bluetooth. Wider ranges of communication ways will bring more security threats such as the sensitive information leakage or malicious attacks.

* Corresponding author. Tel.: +86 13439195095; fax: +86 01067391742.
E-mail address: laiyingxu@bjut.edu.cn (Y. Lai).

http://dx.doi.org/10.1016/j.simpat.2014.02.002
1569-190X/

As MCC is a combination of mobile and CC, the security attacks come from the mobile device, the cloud, and the communication channels. To secure user data and applications, the mobile platform (e.g. Android, iOS, and Windows) providers implemented a variety of different strategies to secure data [4]. However, applying a high level of protection implies a burden on performance and a high level of energy consumption of the mobile device. A commonly used solution for channel security is using SSL protocols. However, these protocols are on one hand high energy consuming and on the other hand provide security properties as a block without taking into account the type of data transmitted or the user expectations for phone applications. On the server side, mobile cloud providers are responsible for securing the data in the cloud and possibly data exchanged between the devices and the cloud. Different solutions have been and are being developed to secure the data access [5,6].

In addition to preventive techniques, security analyses and threat monitoring are essential to the overall security. This paper focuses on mobile cloud security analysis and threat monitoring.

MCC security services should monitor network traffic from mobile users in real time and block any unsecure operation behaviors. Roschke [7] and Vieira [8] summarized users' requirements and proposed an extensible intrusion detection system (IDS) architecture for being easily used in a distributed cloud infrastructure. Dastjerdi [9] proposed a Mobile Agent based IDS which has been customized for CC environment in order to satisfy the cloud user's security requirements. However, due to the frequent changes of user requirements, operation behaviors and other service parameters, it is difficult and expensive to perform a real-time supervision and control in these proposed systems.

Users' traffic behavior and pattern analysis are key techniques for monitoring MCC. There are several challenges on the analysis of the massive users' traffic behaviors: (1) it is difficult to describe user's traffic behaviors because of the complexity of cloud traffic; (2) it is time consuming to analyze massive user's traffic behaviors because of the complex behavior description; and (3) it is time consuming to differentiate and identify individual network user's behaviors from massive network users' data. In order to address these challenges, Farraposo [10] developed a user's traffic behavior analysis method based on the IPFIX protocol. The method was able to detect most of the abnormal behaviors appeared in the network, but could not detect abnormal behaviors which had less impact on the network traffic. Cheng [11] and He [12] used cluster method to define and differentiate the normal cluster from the abnormal ones. When user's traffic behaviors that deviated from the normal cluster exceeded a preset threshold, the user would be considered to be an abnormal user. However, in the real network environment, it is difficult to construct a comprehensive normal traffic behavior's model, which can be used to differentiate different abnormal behaviors. Lakhinaet et al. [13–17] used Wavelet Analysis to detect traffic abnormality in a progressive way. Barford et al. [18] proposed a signal analysis-based network traffic abnormalities. Paxson et al. [19] used a novel statistical method for cloud traffic classification. All these methods were time consuming. To overcome above shortages, a network traffic prediction method based on nonlinear preprocessing was proposed by Yang [20] to detect abnormal traffic behaviors. This method was able to predict the abnormal traffic behavior emerged in network. The shortage was that the threshold needed to be preset, which would either reduce the accuracy or increase false alarm rate based on the value selected. Daihee [21] proposed a network traffic analysis model using online analytical processing (OLAP) on a multidimensional data cube, which provided an easy and fast way to construct a multidimensional traffic analysis system for comprehensive and detailed analysis of traffic data. The threshold needed to be preset too in this approach. Energy conversation is another key domain of study in mobile cloud. Mavromoustakis and Karatza proposed efficient methods in mobile devices for real-time traffic analysis and energy conservation [22,23], and Du et al. studied the energy conservation from cloud side [24].

Although many efforts have been made in traffic pattern collection and analyses, it remains a challenge to analyze massive users' traffic behaviors in terms of accuracy and efficiency. This paper attempts to address the issue by developing a more complete feature set based on the characteristics of network traffic to describe user's traffic behaviors. The method is based on network traffic monitoring and prediction, which can timely detect an abnormal traffic behavior when it emerges and identifies the user who produces the abnormal traffic behavior at the abnormality moment. In addition, the future behavior will be predicted rapidly and accurately.

The proposed method consists of these steps: first, we establish a complete feature set based on the characteristics of network traffic to describe user's traffic behavior. Then, a feature selection rule based on the relative deviation distance is proposed to select the optimized feature sets. We use these feature sets to detect the abnormal traffic behavior. Finally, a traffic behavior analysis method based on prediction is proposed to improve the efficiency of the system. The experimental results show that the proposed method has a higher detection rate and higher efficiency in the analysis of abnormal user's traffic behavior than the existing methods.

The rest of the paper is organized as follows. Representation of network user's traffic behavior and feature selection rule are presented in Section 2. The user's traffic behavior system based on traffic monitoring is given in Section 3. The method based on prediction that is used to analyze the massive users' traffic behavior is studied in Section 4. Finally, the conclusions and future work are given in Section 5.

2. Representation of traffic behaviors and feature selection rules

In MCC, Mobile IP (MIP) is the mobility enabling protocol developed by the Internet Engineering Task Force (IETF) to support global mobility in IP networks. If a mobile host connects to a home network, it is assigned an IP address on its home network, called the mobile host's home address. Packets from a correspondent host to the mobile host are always addressed