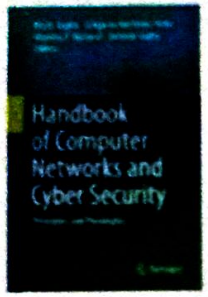


Handbook of Computer Networks and Cyber Security pp 609-634 | Cite as

Investigation of Security Issues in Distributed System Monitoring

Authors | Authors and affiliations

Manjunath Kotari, Niranjan N. Chiplunkar

Chapter

First Online: 01 January 2020

Abstract

The distributed systems have a noteworthy role in today's information technology whether it is

SpringerLink

Investigation of Security Issues in Distributed System Monitoring

Handbook of Computer Networks and Cyber Security pp 609-634 | Cite as

- Manjunath Kotari (1)
- Niranjan N. Chiplunkar (2)

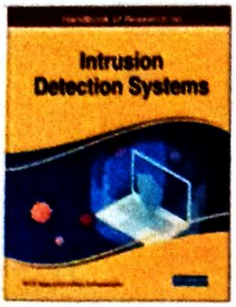
1. AIET, , Moodbidri, India
2. NMAMIT, , Nitte, India

Chapter
First Online: 01 January 2020

Abstract

The distributed systems have a noteworthy role in today's information technology whether it is governmental or nongovernmental organization. Adaptive distributed systems (ADS) are distributed systems that can evolve their behaviors based on changes in their environments (Schlichting and Hiltunen, Designing and implementing adaptive distributed systems, 1998, http://www.cs.arizona.edu/adaptiveds/overview.html (http://www.cs.arizona.edu/adaptiveds/overview.html)). For example, a constant monitoring is required in distributed system to dynamically balance the load using centralized approach (Sarma and Dasgupta, Int J Adv Res Ideas Innov Technol 2:5–10, 2014). A monitoring system or tool is used to identify the changes in the distributed systems and all the activities of the entire network systems. The monitoring of network may help to improve the efficiency of the overall network. However, the monitoring system may be compromised by the intruder by gathering the information from the distributed systems. The various secure and insecure monitoring mechanisms have been adopted by adaptive distributed systems. Most of the distributed systems nowadays use monitoring tools to monitor the various parameters of the networking system. The monitoring tool has been implemented to assess the performance overhead during monitoring. The Wireshark monitoring tool and JMonitor tool (Penteado and Trevelin, JMonitor: a monitoring tool for distributed systems. In Proceedings of international conference on systems, man, and cybernetics, COEX, Seoul, Korea, pp 1767–1772, 2012) have been used to monitor the communication between the various users and also to monitor the computational resources used in networked computers. The main concern of this chapter is to investigate the existing monitoring tools for finding the impacts of monitoring activities in the distributed network. The investigations result that, when the monitoring tool collects security-critical information, there is a high risk of information disclosure to unauthorized users. The second concern is that a secure communication channel can be implemented by using the Rivest, Shamir, and Adelman (RSA) algorithm to monitor the confidential information. This chapter illustrates the implementation and experimental results related to authors' research work and formulation of framework for security mechanisms in the context of adaptive distributed systems (Kotari et al., IOSR J Comput Eng 18:25–36, 2016).

Security issues for existing monitoring tool are investigated in detail here. In this connection, the chapter deals with the several security-related network scenarios experienced during monitoring with the help of Wireshark monitoring tool. The proper use of Wireshark monitoring tool helps to identify the possible security threats such as emerging threats of hackers, corporate data theft, and identifying threats due to viruses. The implementation of secure communication channel is discussed, which minimizes the above set of threats.



A Survey on Detection and Analysis of Cyber Security Threats Through Monitoring Tools

Manjunath Kotari (Alva's Institute of Engineering and Technology, Moodbidri, India) and Niranjan N. Chiplunkar (NMAM Institute of Technology, Nitte, India)

Source Title: Handbook of Research on Intrusion Detection Systems (/book/handbook-research-intrusion-detection-systems/235719)

Pages: 28
DOI: 10.4018/978-1-7998-2242-4.ch005

Abstract

Cyber crime is a serious threat for day-to-day transactions of the digital life. Overexposure of the personal details in social networks will lead to the cyber crime case. Therefore, detection and monitoring of cyber crime are challenging tasks. The cyber criminals are continually flooding the various intrusions all over the network. The cyber safety team should have a noteworthy challenge of filtering various such information. Continuous nonstop cyberattacks or intrusion examinations by security tools will significantly improve the threat alerts. However, cyber security becomes more expensive in the case of the above methods. The chapter provides systematic survey of various cyber security threats, evolution of intrusion detection systems, various monitoring mechanisms, open source cyber security monitoring tools, and various assessment techniques. The chapter also proposes a model of Cyber security detection and monitoring system and its challenges.

Chapter Preview

Top

1. Introduction

Cyber security threats are major hurdle for the development activities of the Information Technology (IT) industry. The IT industry is facing severe crisis of cyber-crime activities in their business. A large set of data and assets of organizations are placed in cloud-based platform. The virtual cloud computing is facing various threats which include, Intrusions, Malwares, and Mining of Crypto currency. The Virtual Machines faces intrusions and impersonations in the cloud environments. The bitcoin attracts more severe cyber crimes. This can be illustrated in cloud computing by layer wise cyber attacks. Cyber Security (Gupta, Agrawal, & Wang, 2019) is becoming a very important concern for the functioning of web applications. The rising cost of cyber security damages reflects a failure of the security field to offer a solution that is both simple enough to warrant adoption by industry and government and secure enough to protect our valuable assets and data. Most of the organizations are facing shortage of cyber security professionals to monitor the user activities in day to day life. However, IT organizations may use various tools and technologies to maintain privacy of user data. Most of the corporate information security (Quhtani, 2017) is analyzed by data mining applications. In the corporate world, marketing campaign surveys are analyzed according to data mining applications. The objective of this chapter is to provide the comprehensive survey on detection and analysis of various cyber security threats exists in the web applications and network. The chapter also reviews the various open source security monitoring tools with classifications. The challenges faced by cyber-security tools have been included for the purpose of providing future solutions. The architecture of cyber-security threat detection and monitoring system to analyze the working of cyber-security tools has been proposed in this chapter.

1.1 Cyber Security Monitoring

Security monitoring is the collection of data from a range of security systems and the correlation and analysis of this information with threat intelligence to identify signs of compromise. Cyber-Security monitoring is an essential part of cyber risk management systems, which enables the company networks to detect cyber hackers in their early life, and quickly shoot up threats for healing before they cause harm and interference. Baselining is the process of establishing an agreed level of typical network performance. It plays an important role in cyber security monitoring. Any network behavior that falls outside what is considered regular behavior should be analyzed to identify whether or not it could be malicious.

1.2 How Does Cyber Security Monitoring Work?

Cyber security analysts will utilise a range of technologies to achieve visibility of threats. There are two types of monitoring, viz., network security monitoring and endpoint security monitoring. Network security monitoring tools comprise Security Information and Event Management (SIEM) and Intrusion Detection Systems (IDS). SIEM systems collect, manage and correlate log information from a range of sources to provide a holistic view of security posture, and generate alerts for investigation by cyber security analysts. IDS combines network (NIDS) and host (HIDS) based methods to analyse network traffic and identify anomalous behaviour. Endpoint security monitoring technologies provide visibility of activity such as file read, write, executions and registry changes across desktops, laptops, and servers.

1.3 Challenges of In-house Security Monitoring

Chapter 5
A Survey on Detection and Analysis of Cyber Security Threats Through Monitoring Tools

Manjunath Kotari
Alva's Institute of Engineering and Technology, Moodbidri, India

Niranjan N. Chiplunkar
NMAM Institute of Technology, Nitte, India

ABSTRACT

Cyber crime is a serious threat for day-to-day transactions of the digital life. Overexposure of the personal details in social networks will lead to the cyber crime case. Therefore, detection and monitoring of cyber crime are challenging tasks. The cyber criminals are continually flooding the various intrusions all over the network. The cyber safety team should have a noteworthy challenge of filtering various such information. Continuous nonstop cyberattacks or intrusion examinations by security tools will significantly improve the threat alerts. However, cyber security becomes more expensive in the case of the above methods. The chapter provides systematic survey of various cyber security threats, evolution of intrusion detection systems, various monitoring mechanisms, open source cyber security monitoring tools, and various assessment techniques. The chapter also proposes a model of Cyber security detection and monitoring system and its challenges.

1. INTRODUCTION

Cyber security threats are major hurdle for the development activities of the Information Technology (IT) industry. The IT industry is facing severe crisis of cyber-crime activities in their business. A large set of data and assets of organizations are placed in cloud-based platform. The virtual cloud computing is facing various threats which include, Intrusions, Malwares, and Mining of Crypto currency. The

DOI: 10.4018/978-1-7998-2242-4.ch005

Source details

International Journal of Advanced Science and Technology

Scopus coverage years: from 2016 to 2020

(coverage discontinued in Scopus)

Publisher: Science and Engineering Research Support Society

ISSN: 2005-4238 E-ISSN: 2207-6360

Subject area: Energy: General Energy | Computer Science: General Computer Science | Engineering: General Engineering

Source type: Journal

CiteScore 2019
0.0

SJR 2019
0.108

SNIP 2020
0.596

View all documents > | Set document alert | Save to source list | Source Homepage

CiteScore | CiteScore rank & trend | Scopus content coverage

Improved CiteScore methodology

CiteScore 2019 counts the citations received in 2016-2019 to articles, reviews, conference papers, book chapters and data papers published in 2016-2019, and divides this by the number of publications published in 2016-2019. Learn more >

CiteScore 2019

$$0.0 = \frac{35 \text{ Citations } 2016 - 2019}{1{,}437 \text{ Documents } 2016 - 2019}$$

Calculated on 06 May, 2020

CiteScore rank 2019

Category	Rank	Percentile
Energy General Energy	#61/63	3rd
Computer Science General Computer Science	#217/221	2nd
Engineering		

View CiteScore methodology > | CiteScore FAQ > | Add CiteScore to your site

International Journal of Advance Science and Technology
Vol. 29, No. 10S, (2020), pp. 7671-7676

Management in Centralized MANET's using Layered Coding Techniques

Sushant Mangasuli[1], Dr. S. Mohideen Badhusha[2], Arundhati Nelli[3], Ranjana Battur[4]

[1,2]Departmnet of CSE Alva's Institute of Engineering and Technology,Moodbidri, India,
[3,4]Departmnet of CSE KLS Gogte Institute of Technology, Belagavi, India
sushantm04@gmail.com[1], badhusha.sm@gmail.com[2], avnelli@git.edu[3], rbbattur@git.edu[4]

Abstract

The resource utilization problem has been considered broadly over wired and wireless networks and it is known to be NP hard. However, due to the high mobility of peers and current network conditions, the resource allocation problem is common issue. Most of the carried research considers streaming the videos to the destination node using a single source and without implementing any coding techniques which introduces huge playback issue. Moreover, in the context of MANETs, the resource utilization adds new challenges as nodes are considered to have limited energy with a highly dynamic topology. This paper explores and compares the resource utilization problems over MANETs using coding techniques and energy efficient routing algorithms to efficiently utilize the available resources in the network.

***Keywords**: SVC, MDC, Video Coding Techniques, Energy Efficient Routing*

1. INTRODUCTION

Mobile adhoc network (MANET) is an assembly of wireless mobile nodes arranged to communicate with each other without the support of any fixed infrastructure. They are similar to P2P networks, and are considered to be self-adaptive, self-configurable and self-manageable. These networks can be a mobile phone, tablet, PDA or any personal device with a wireless interface and has a tendency to join a wireless network. MANETs are encompassed of several wireless technologies such as 802.11 WLAN, Bluetooth, 3G and 4G, etc. MANETs are widely used in situations where it is difficult to provide any fixed infrastructure. In [1], the authors have identified a number of applications where MANETs are a valuable solution such as; emergency situations, unplanned crowd, disaster recoveries and over the military applications. Hence, it is a major requirement of any protocol designed to consider the energy efficiency as a primary objective. It is even more important to look at energy when video distribution or streaming over MANETs. An significant increase in QoS technique in MANET's for real-time data transmission has been presented in [2] keeping in sight multimedia transmission as management of distributed control plane with various controllers and each controller achieves few QoS task. For effective multimedia transmission is concerned, it has always challenging task in wireless networks due to node mmobility, changeable network conditions, heterogeneous network configurations and QoS issues. [3,4].

2. LITERARURE REVIEW

Streaming video over MANETs is among one of the most challenging issues [5]. It is usually affected by heterogeneous uplink bandwidth of nodes, interference, transmission power for the nodes, node mobility, collision, playback latency, multipath fading and dynamic change in topology etc. Hence, the overall challenge becomes to improve the Quality of Experience (QOE) among users throughout the multimedia session. This can be achieved if the network has enough bandwidth available and can able to maintain latency. MANETs rely on the participating nodes in the network to share the resources among each other. This adds further challenge to the network to maintain and discover the optimal routes because of the mobility nature of the nodes. Hence, in order to solve his issue a wide range of routing techniques required [6]. The possible issues in Mobile adhoc Networks for streaming the video are listed below [7]:

ISSN: 2005-4238 IJAST