International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 01 (January- February, 2018)

Consequences of Malicious Nodes in Mobile Social Cloud Computing: An Analysis

Kiran Patidar
Ph.D Scholor, Department of CSE
AISECT University, Bhopal, India
kiranpatidar21@gmail.com

Priti Maheshwary
Ph.D Scholor, Department of CSE
AISECT University, Bhopal, India
pritimaheshwary@gmail.com

Piyush Kumar Shukla
Assitant Professor, Department of CSE
RGPV, Bhopal, India
pphdwss@gmail.com

Anand Motwani
Assitant Professor, Department of CSE
SISTec-R, Bhopal, India
motwani.personal@gmail.com
*

Abstract— *In recent years, developers build abundant mobile applications in various domains such as entertainment, sports, social networking, business, news and travel. The convergence of mobile computing, social networking and Cloud Computing (CC) gave birth to a new and powerful paradigm of pervasive computing i.e. 'Mobile Social Cloud Computing' (MSCC), for achieving great interaction. Mobile devices in MSCC create SNs, which is based on basic authentication, to share cloud services. MSCC has some distinctiveness that differentiates it from usual Grid computing. Though, there are many issues in MSCC due to the behavior of mobile devices that must be handled. One such behavior is malicious behavior. Malicious in this paper includes all user acts that only use cloud services from other users and avoid providing cloud services to others. Most of the schemes are proposed against random faulty clouds and works well, but these do not protect from malicious nodes present in clouds. In this work, the affects of malicious nodes on quality of service (QoS) parameters are presented to pioneer towards development of fault tolerant algorithms.*

Keywords— Cloud Computing, Content Addressable Network (CAN), Fault tolerance, malicious nodes, Mobile Social Cloud Computing (MSCC), Pervasive Computing, Quality of Service (QoS), Scheduling, Security, Social Networking, Privacy, Virtualization.

I. Introduction

In the recent years, we have seen that CC frameworks, such as AWS (Amazon Web Services) [2], Microsoft Azure [3] and Google App Engine [4] become progressively more popular among IT developers and organizational clients. Mobile Social Cloud Computing (MSCC) [1, 5] integrates the Cloud Computing [8] and Social networking into the wireless mobile communication environment. We have seen an exceptional boost in the usage and deployment of smart phone platforms and social networking applications worldwide. Social Networking Service (SNS) [6] is platform provided by an application, where people with similar interests, family and friends connect with each other to communicate and share the data. In social computing, users share media and other files among each other with less or no authentication because users are eager to provide their data to other SN members even through mobile devices. Another reason of using SNS nowadays is to promote the businesses and to reach out more and more people and communities. It has significantly impacted people's lives in every aspect: from social to personal as they regularly share and communicate on social networks (SNs). The utilization of SNS is really soaring with increased use of wireless mobile devices [1].

In the SNS, malicious users are those who take cloud services from other devices and shun providing services to others due to one or the other reason [1]. Malicious users may reject another's request when getting a request for cloud services from another user or disconnect another user forcibly even while providing cloud services to another user. Malicious nodes affect the QoS at much greater extent. Here, in this work, the affects of such nodes on certain QoS parameters [9] is studied.

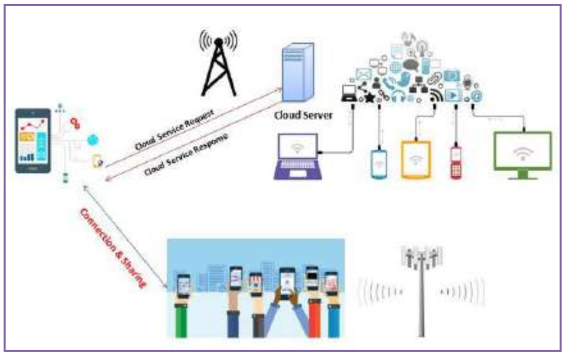


Fig. 1: Connection and Sharing in MSCC Environment

II. SCC Environment

MSCC can address the faults (problems frequent disconnections due to resource scarcity and mobility) by executing mobile applications on providers external to the mobile device [7]. Figure 1 shows the MSCC computing environment and communication format over MSCC. MSCC is using Content Addressable Network (CAN) which is type of Peer-to-Peer network. For instance User-1 and User-2 are on same social network. When User-1 requests cloud service from server, the server returns address of device of user 2 from within the same social network of user 1.Finally both user connect and share the resources and / or services, without much authentication. Also a mobile device can be a member of any or every social network.

III. EXPERIMENT

The simulation environment, for experimenting with MSCC, is configured in famous CloudSim [10] tool. The algorithm for malicious node deployment in MSCC and other objects are instantiated for MSCC.

3.1 Simulation Scenario and Configuration

The network chosen for experimentation is with CAN, as it is just to define logical structure of Mobile Networks. CAN structure does not influence either QoS scheduling performance or fault tolerance [1]. The simulation scenario for experimentation purpose and configuration is given in Table 1 and 2 respectively.

Table 1: Simulation Scenarios

Case No.	SNS	With Malicious Node
Case 1	Yes	No
Case 2	Yes	Yes

Table 2: Simulation Configuration

Entiities	Numbers
Data Centre	03
Broker	04
Virtual Machine	30
Hosts(Mobile Devices)	100
Cloudlet (Varying length)	50
VMM	Xen

VM Configuration	RAM=512,
	MIPS=250,
	PEs=01

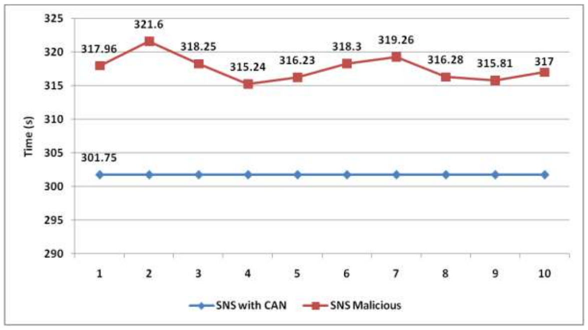


Fig.2: Effect of Malicious Nodes on Execution Time in SNS

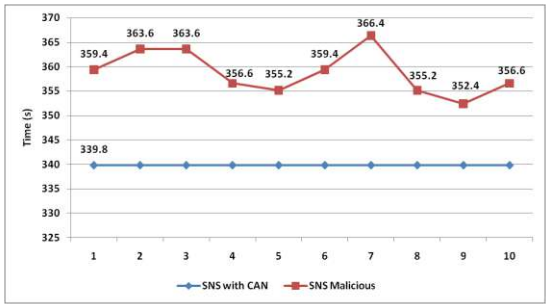


Fig. 3: Effect of Malicious Nodes on Finish Time in SNS

IV. CONSEQUENCES OF MALICIOUS NODES IN SNS: AN ANALYSIS

To see the effects of Malicious Nodes in SNS, 02 cases mentioned in Table 1 are simulated and results are listed in Table 3. The results of 10 experiment runs out of 50 are taken. The average number of malicious nodes is approximately 50% in the environment.

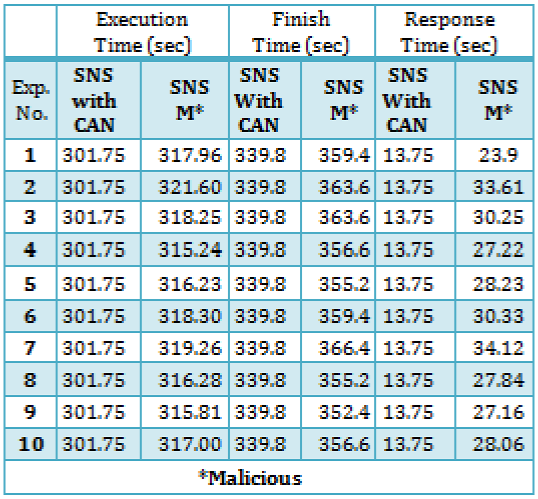
4.1 Cloud Service Execution Time

It is referred to as time taken to execute the service that is requested by mobile device. Figure 2, showing the effects of malicious nodes on execution time.

4.2 Cloud Service Finish Time

Finish Time represents the end of all tasks running at DC. It is also represented as Maximum Turnaround time taken by a process. In Figure 3, effects of malicious nodes on finish time, is shown.

Table 3: Comparison of QoS Performance Parameters



	Execution Time (sec)		Finish Time (sec)		Response Time (sec)	
Exp. No.	SNS with CAN	SNS M*	SNS With CAN	SNS M*	SNS With CAN	SNS M*
1	301.75	317.96	339.8	359.4	13.75	23.9
2	301.75	321.60	339.8	363.6	13.75	33.61
3	301.75	318.25	339.8	363.6	13.75	30.25
4	301.75	315.24	339.8	356.6	13.75	27.22
5	301.75	316.23	339.8	355.2	13.75	28.23
6	301.75	318.30	339.8	359.4	13.75	30.33
7	301.75	319.26	339.8	366.4	13.75	34.12
8	301.75	316.28	339.8	355.2	13.75	27.84
9	301.75	315.81	339.8	352.4	13.75	27.16
10	301.75	317.00	339.8	356.6	13.75	28.06
*Malicious						

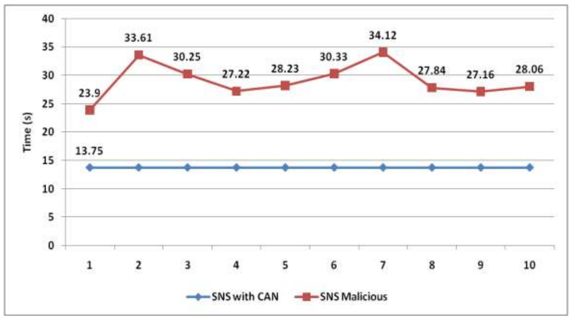


Fig. 4: Effect of Malicious Nodes on Response Time in SNS

4.3 Cloud Service Response Time

It refers to the time which is elapsed between submission of service request and time when application or host starts response. In other words, the time of beginning of the first service execution is known as response time. In Figure 4, the effects of malicious nodes on response time, is shown.

4.4 Analysis

After analyzing the results as depicted in Figures 2 to 4, following Observations has been done:

1. The execution time is increased by 65% in malicious environment.
2. The Finish time is increased by 78% in malicious environment.
3. The response time in increased by 1.5 times the normal response time.

V. Conclusion & future work.

In most of the previous works referred the severity of malicious behaviour of nodes did not analyzed. It is must to consider malicious nodes in SN based on MSCC as it is common phenomenon by nodes to misbehave or act maliciously. In this work, a detailed analysis of effects, imposed by malicious behaviour of nodes in MSCC, is presented. MSCC essentially includes another user requirement i.e. QoS. QoS is necessary metric to evaluate the quality of MSCC. Depending on the research areas, different researchers defined QoS in different ways. Time and Cost are considered in basic QoS while reliability, availability, security/privacy, and reputation covered in extended QoS. In this work, affects of malicious nodes over certain metrics are studied. In literature, to exclude such users, mobile device reputation function is used. As a future work, effects of such nodes on extended parameters can also be studied to develop effective fault tolerant scheduling algorithms. The work also motivates to build a system to evaluate the accuracy of fault tolerant algorithms.

REFERENCES

[1]. Sook Kyong Choi, KwangSik Chung and Heonchang Yu "Fault Tolerance and QoS Scheduling using CAN in Mobile Social Cloud Computing", Springer Cluster Computing, DOI 10.1007/s10586-013-0286-3, 2013.

[2]. Amazon. Amazon Elastic Compute Cloud (EC2). http://aws.amazon.com/ec2/.

[3]. Microsoft Windows Azure. http://www. microsoft. com /windowsazure/.

[4]. Google, Google Apps. http://www.google.com/apps/.

[5]. Zohreh Sanaei, Saeid Abolfazli, Abdullah Gani, and Rajkumar Buyya, "Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 1, FIRST QUARTER 2014.

[6]. E.E. Marinelli, Hyrax: cloud computing on mobile devices using MapReduce, Masters Thesis, Carnegie Mellon University, 2009.

[7]. Niroshinie Fernando, Seng W. Loke, Wenny Rahayu, "Mobile cloud computing: A survey", Future Generation Computer Systems 29 (2013) 84–106.

[8]. Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu, "Cloud Computing and Grid Computing 360-Degree Compared", Available at: https://arxiv.org/ftp/arxiv/papers/0901/0901.0131.pdf

[9]. Qian, T., Huiyou, C., Yang, Y., Chunqin, G.: A trustworthy management approach for cloud services QoS data. In: ICMLC, pp.1626–1631 (2010)

[10]. Rodrigo, N.C., Rajiv, R., Anton, B., De Rose, C.A.F., Buyya, R.: CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. SPE J. 41(1), 23–50. ISSN:0038-0644 (2011)

Author's Profile

Kiran Patidar is pursuing her Ph.D. in Computer Science and Engineering. She is currently a PhD Scholar at AISECT University, Bhopal, India. She is a brilliant academician and researcher who brought with her the rich academic experience. She has 3 years of experience with renowned educational institutions and attended national level conferences, workshops, seminars and FDPs. She has attended workshop at IIT Mumbai for C and C++. Her domain of expertise includes: Software Engineering, Cloud Computing and Data Structures

Priti Maheshwary is an Associate Professor in Computer Science and Engineering department at AISECT University, Bhopal. She had her Doctorate from MANIT, Bhopal in Remote Sensing Image Retrieval. She has completed research project on Climate Change detection and monitoring funded by SAC and Environment Monitoring using Sensor devices funded by AISECT University. Ongoing Project is on Crop Monitoring sponsored by SAC. She is the author of more than 20 publications in different journals of repute out of which two journal papers and two conference papers on IoT. She is the author of book chapter on Software Copyright. Her interests include Internet of Things, Cyber Physical Systems, Mobile Networks, WSN, Adhoc Networks, Data mining, and Image Processing. Her work experience includes 20 years in teaching computer science and engineering. She is guiding PhD in the field of image processing, IoT and Networks.

Dr. Piyush Kumar Shukla: received his Bachelor's degree in Electronics & Communication Engineering, LNCT, Bhopal in 2001, M.Tech (Computer Science & Engineering) in 2005 from SATI, Vidisha and Ph.D. (Computer Science & Engineering) in 2013 from RGPV, Bhopal. M.P. India. He is a Member of ISTE (Life Member), IEEE, ACM, Member of IEEE-'Cloud Computing', IEEE-'Internet of Things' Society and ORCID, ReserchGate, IACSIT, IAENG. Currently he is working as an Assistant Professor (Academic Grade

Pay-8000) in the Department of Computer Science & Engineering, UIT-RGPV Bhopal. He is also I/C of PG Program (Dual Degree Integrated PG-Programs) in DoCSE, UIT, RGPV, Bhopal, Madhya Pradesh, Bhopal. He has published more than 50 Research Papers in various International & National Journals & Conferences, including 04 Papers in SCIE Journals & More than 10 papers in Scopus Journals.

Anand Motwani pursuing his Ph.D. in Computer Science and Engineering. He is currently an Associate Professor and Head at Sagar Group of Institutions (SISTec-R), Bhopal, India. He is member of IEEE-'Cloud Computing', IEEE-'Internet of Things' Society and ORCID. He is a brilliant academician and researcher who brought with him the combination of both industry as well as rich academic experience. He has over a decade of experience with renowned educational institutions and industries and attended several national level conferences, workshops, seminars and FDPs. He has published an engineering book with Pearson Education and also published and presented several papers in quality conferences and journals. His domain of expertise includes: Software Engineering, Cloud Computing, Data Analytics, Machine Learning and Wireless Networking.