**IJCTA**, 9(27), 2016, pp. 329-334 ISSN: 0974-5572
© International Science Press

# Seamless traffic congestion during data transfer on Network in Mobile Cloud Computing Using RED & CADA

**S. Jany Abiraham* and J.G.R. Sathiaseelan****

**ABSTRACT**

The Mobile device is growing at an extremely high speed. Everyone has a mobile device with network facility. Hence in the day to day life the Mobile usageis widening. In mobile cloud computing, there are several kinds of issues. One of the issues is network related issues. In the paradigm traffic congestion is one the drawback of the network issuesduring the traffic congestion, it reduces the quality of service of the network and also drops the packets it causes the re-transmission. During re-transmit it requires more cost and more bandwidth. It also checks the particular destination node is available or not. For each transaction an amount of data stands in a queue. To overcome the traffic congestion using Random Early Detection and Context Aware Decision algorithm is implemented.

***Keywords:*** Mobile Cloud Computing, Traffic Congestion, Security, Network Issues

## 1. INTRODUCTION

The speedy growth of mobile computing becomes a dominant tendency in the progress of ITas well as trade and manufacturing fields[2]. However, the movable strategy is facing many challenges in their funds and infrastructure[4]. The incomplete capitals considerably hold up the development[1] of service behavior. Cloud computing has been broadly familiar as the next generation's computing communications[5]. Cloud Computing offers a number of compensation byallowing users to use transportation, platforms, and software[6]. To reduce the distribution postponement, it is desirable to decrease to come instance[9] throughout the distribution. The best development is the purpose nodes wake up directly when the resource nodes gain the distribution packets. Based on this, a level-by-level counterbalance agenda is planned[10]. Hence, it is likely to attain low broadcast holdup[15] with node-by-node compensate agenda in multi-hop WSNs. It is still a face for us to be relevant the level-by-level counteract to fright distribution[11] in the serious occurrence monitoring. First the order of nodes wake should have confirmed by using the transfer way[7]. If the traffic run is in the conflicting direction the wait in each hop will be as big as the span of the whole responsibility cycle. Second the level-by-level counterbalance working by the pack giving out could reason a grave conflict.

## 2. RELATED WORK

[1] As mobile computing has been urbanized for ten years, a fresh replica for portable computing, that is, mobile cloud computing, emerges consequential from the wedding of great so far reasonably priced portable devices and cloud computing. Here, review obtainable portable cloud computing applications, as well as wonder prospect creation mobile cloud computing applications. It gives insights for the enabling technologies and challenges that lie in front for us to shift forward from MC to MCC for constructing the next invention portable cloud applications. For each of the challenges, it gives a review of presented solutions, classify investigate gaps, and put forward potential investigate areas.

* Research Scholar, Department of Computer Science, Bishop Heber College Tiruchirappalli, Tamilnadu, India, *Email: jani.mellu5021@gmail.com*

** Head, Department of Computer Science, Bishop Heber College Tiruchirappalli, Tamilnadu, India, *Email: jgrssathiaseelan@gmail.com*

[2] In few years back jointly with a volatile enlargement of the portable applications and rising of cloud computing notion has become one of the manufacturing hum words and a main conversation fiber in the IT world since 2007. Mobile cloud computing combines the cloud computing into the movable surroundings and overcome obstacles related to the performance, environment and security in mobile computing. This shows the key open investigate issues linked with the movable usage of cloud computing which helps universal readers to have an impression of the MCC, their issues, existing solutions and methods.

[3] To improve the safety of mobile cloud users, a few proposals have been obtainable in recent times.Though argue that most of them are not appropriate for portable cloud where portable users power join or leave the mobile networks randomly. Here, this design a protected portable user-based data service mechanism to provide isolation and fine-grained access control for information stored in the cloud. This process makes the mobile users to enjoy a protected outsourced data services at a minimized safetymanagement in the clouds.

[4] Despite growing usage of mobile computing, exploit its full potential is difficult due to its inherent problems such as resource shortage, recurrent disconnections, and mobility. Mobile cloud computing can address these troubles by executing mobile application on resource providers outside to the mobile device. To provide an extensive survey of mobile cloud computing investigate, while importance the specific concerns in mobile cloud computing. A taxonomy base on the solution issue in this region, and discuss the dissimilar approaches taken to tackle these issue. To conclude the paper with a critical analysis of challenge that have not yet beenfully met, and highlight guidelines for future work.

[5] Mobile Cloud compute usually consists of front-end users who possess mobile devices and back-end cloud servers.This prototype empowers users to pervasively access a large amount of storage resources with transportable devices in a distributed and supportive manner. During the period between uploading and downloading files (information), the isolation and integrity of files need to be assured. To this end, families of scheme are proposed for dissimilar situations. All schemes are lightweight in terms of computational overhead, elastic to storage compromise on mobile devices, and do not think that trusted cloud servers are present. Matching algorithms are proposed in detail for guiding off-the-shelf execution. The evaluation of safety and performance is also lengthily analyzed, justifying the applicability of the proposed scheme.

The center of this study, based on obtainable journalism, is to define a method for cloud provider that will guard users' data, information which is of high importance.

[6] In cloud computing highly scalable computing assets are supplied as an external service through internet on pay-as-usability basis. Portico examine estimate that mobile subscribers will reach 6.5 billion by the end of 2012, 6.9 billion by the end of 2013. Due to rising use of mobile devices the requirement of cloud computing in mobile devices arise, which give delivery to Mobile Cloud Computing (MCC). MCC refers to an infrastructure where data processing and storage space can happen away from mobile device. Mobile devices do not need to have big storage space capacity and powerful CPU speed. Due to store information on cloud there is an issue of data security. Because of the risk connected with information storage many IT professional are not presentation their attention towards Mobile Cloud Computing. This paper explores: (i) The idea of Mobile Cloud Computing and issues linked in it (ii) protection of information stored in cloud with various mechanisms (iii) Proposed a possible answer to provide privacy, access control as well as honesty of data.

## 3. ISSUES

Cloud is very dominant to perform computations while computing ability of mobile devices, has a limit. so many issues occur to show inability to transferring data and executing time. So there are some issues in implementing cloud compute for mobile. These issues can be related to restricted resources, connected to network, related to seamless network connectivity during data transferring.Some issue is explained as follows like Network Related Issues. So this issue such as connected to the network like Bandwidth, latency, availability and heterogeneity. The majority of mobile devices have almost same functionalities like a desktop computer. The movable devices also have to face a number of problems related to traffic congestion. So analyze the problem to find, then overcome this problem one the network.

## 4. ENHANCED SYSTEM

### 4.1. Overview of The Proposed System

In this proposed system to utilize RSUs to route packets to distant locations.A vehicle S requesting to send a packet P to a far-away vehicle D can throw P to its nearest RSU (R1), which, in turn, sends P to the nearest RSU to D (R2) through the RSU system. R2 then send P to D through multihop. Carry and forward mechanisms for Dependable message delivery in VANET using RSUs and RED algorithm(CAN DELIVER). The design of this system is divided into two basic parts: the first part rule routing from a medium to its adjacent RSU, and the second part handles routing from RSUs to vehicles. And also using Context Aware Decision algorithm is implemented.

### 4.2. Red Algorithm

The Random early detection (RED), also known as random early discard or random early drop is queuing for a network scheduler apt for congestion avoidance. RED is more fair than tail drop, in the sense that it does not have a bias against burst traffic that uses only a little portion of the bandwidth. The more a host transmits, the more probable it is that its packet are dropped as the likelihood of a host's packet being dropped is proportional to the quantity of information it has in a line. In the early hour's discovery helps avoid TCP global synchronization.

```
Initialization
    $avg \leftarrow 0$
        $Count \leftarrow -1$
    For each packet arrival
    If the queue is non-empty
        $avg \leftarrow (1- \omega_q) \times avg + \omega_q \times q$
    else
        $m \leftarrow f(time - q\_time)$
        $avg \leftarrow (1-\omega_q)^m \times avg$
    If $min_{th} \leq avg < max_{th}$
        Increment count
$Pb \frac{avg - min_{th}}{max_{th} - min_{th}} max_p$
    $Pa \frac{Pb}{1 - count\ x\ Pb}$
With probability Pa :
    mark the arriving packet
    $count \leftarrow 0$
Else if $max_{th} < avg$
    mark the arriving packet
    $count \leftarrow 0$
Else $count \leftarrow -1$
When queue become empty
    $q\_time \leftarrow time$
```

### 4.3. Context Aware Decision Algorithm

To consider the decision engine of mobile cloud offloading systems, this decides whether to offload a given method to the cloud servers. To design, execute, and evaluate a context-aware decision algorithm, called CADA, to optimize the presentation of the mobile devices with a variety of optimization criteria, including short reply time and low energy consumption. The CADA algorithm can vocation with a variety of mobile cloud offloading system proposed in the writing. We have implemented the CADA algorithm and included it with Thin Air, and conducted experiments with actual Android users. The evaluation outcome exposes that: (i) the importance of a context-aware decision engine, (ii) the high calculation correctness of the CADA algorithm, (iii) the presentation upgrading (in both reaction time and energy expenditure) achieved by the CADA algorithm, and (iv)the insignificant slide incurred by the CADA algorithm and other software mechanism in our organization. In adding up to the CADA algorithm, we also expand a background aware power sculpt for mobile strategy, which is of pleasure in its own correct.

## 5. EXPERIMENTAL EVALUATION AND RESULT MODULES

### 5.1. Vehicle-to-vehicle (V2v) And Vehicle-to-infrastructure

In this Module, the two basic statement modes, which correspondingly allow OBUs to communicate with each other and with the infrastructure RSUs. Since vehicles correspond during wireless channels, an assortment of attacks such as injecting fake in sequence, modifying and replaying the dispersed communication can be simply launched.A security attack on VANETs can have severe harmful or fatal consequences to justifiable users. Consequently, ensuring protected vehicular communications is a must facing any VANET request can be put into observe.A well-recognized solution to secure VANETs is to deploy Public Key Infrastructure (PKI), and to employ Certificate Revocation Lists (CRLs) for organization the revoked record. In PKI, each entity in the network holds a genuine credential, and every memoshould be digitally signed before its transmission. A CRL, typically issued by a Trusted Authority (TA), is a list containing the entire revoked certificate. In a PKI scheme, the authentication of any communication is performed by first checking if the sender's certificate is included in the current CRL, i.e., examination its revocation position, then, verifying the sender' certificate, and finally verifying the sender's signature on the received message.

### 5.2. Routing From Vehicle to Nearest Rsu

When a vehicle S requirement to propel a package P to an RSU R, it examines whether R is within its transmission range (r). If so, S sends P straight during the wireless conduit. In this project proposes that the shortest path between any two intersections can be considered and stored so that vehicles use them when sending packets. Hence, we suggest deploying a virtual waypoint at each junction.To validate the proposed scheduling scheme in real wireless communication environment.

### 5.3. Keep Time Synchronous

After broadcasting the assignment, the center node begins to send beacon in its sending time slot and sleeps according to its sleep scheduling. Each neighbor receiving the beacon actually gets a reference of time, and it relays the beacon in its sending time slot assigned. In this way, all nodes will begin to work in a duty cycle way. Every 10 minutes, the center node transmits a beacon in its sending time slot, and its neighbors receiving the beacon will adjust their timers according to the beacon if there is an error of synchronization due to clock drift in this way, local time synchronization in the network is maintained.

### 5.4. Record The Communication Delay

To obtain the result of broadcasting delay in the network, a mobile node carried by a person is used for results collection. Each node records the time when it receives the alarm and sends its record to the mobile node when the

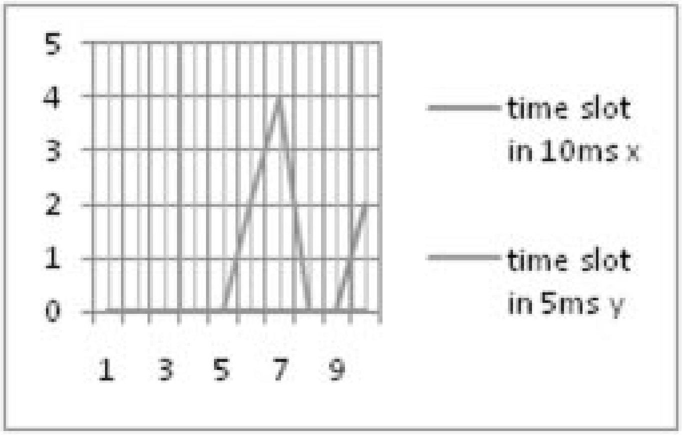

**Figure: Shows that the result of the experiments**

mobile node inquires it. The alarm is originated by an arbitrary node selected in the network. It made 10 experiments and recorded the maximum broadcasting delay in the network. The duty cycle is set to be 1*s*. Figure: shows the experiment results. The red line stands for results when time slot is 5*ms*, and the blue line stands for results when time slot is 10*ms*. It can be seen, the predictable system achieves very low distribution delay (0.06*s*) in most of the experiments when time slot is 5*ms*, except for experiment 6 and 7. In experiment 6, the case that packet cannot be successfully transmitted within 5*ms* took place once in the alarm broadcasting, resulting in an extra delay of two duty cycles, i.e., 2*s*. In experiment 7, the case took place twice. When we increased the size of time slot to be 10*ms*, the performance of the proposed scheme becomes better, as shown in Figure.

## 6. CONCLUSION AND FUTURE WORK

Mobile cloud computing is mobile environments trends in the prospect since it integrates the benefits of both mobile computing and cloud computing, in that way giving best services for mobile users. The condition of mobility in cloud computing gave origin to Mobile cloud computing. It gives more potential for contact services in suitable way. It is predictable that following a number of years some mobile users will go to use cloud computing on their mobile devices. According to a current revise by ABI investigate, a New York-based rigid, more than 240 million trade will use obscure services during portable devices by 2015.The attraction will drive the income of portable cloud computing. With this meaning, this has given an impression of mobile cloud computing in which its definitions, safety, issues and benefits have been prospected. Mostly it discussed regarding safety of information stored in cloud and meaning of information security. This has explored some mechanisms for given that information safety. so that Mobile Cloud Computing can be broadly established by some users in prospect. It also planned a method to offer privacy, contact control as well as reliability to mobile users.

## REFERENCES

[1] Portio Research, “Mobile subscribers worldwide,”*http://www.onbile.com/info/mobile subscribers-worldwide.*

*[2] DhammapalTayade,research student “Mobile Cloud Computing:network related issues, security advantages, trends”(IJCSIT) International Journal of Computer Science and Information Technologies,**5(5)**,2014 .*

[3] White Paper, *Mobile Cloud Computing Solution Brief. AEPONA*,2010.

[4] Hoang T. Dinh, Chonho Lee, DusitNiyato, and Ping Wang, “Asurvey of mobile cloud computing: architecture, applications, andapproaches,” *Accepted in Wireless Communications and Mobile Computing - Wiley.*

[5] Abdul Nasir Khan, M.L. Mat Kiah ,Samee U. Khan, Sajjad A.Madani , “Towards secure mobile cloud computing: A survey,”*Future Generation Computer Systems*,2012.

[6] W. Itani, A. Kayssi, A. Chehab, “Energy-efficient incrementalintegrity for securing storage in mobile cloud computing,” *in: Proc. Int. Conference on Energy Aware Computing, ICEAC ’10, Cairo, Egypt*, 2010.

[7] W. Jia, H. Zhu, Z. Cao, L. Wei, X. Lin, “SDSM: a secure dataservice mechanism in mobile cloud computing,” *in: Proc. IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, Shanghai*,2011.

[8] J. Yang, H. Wang, J. Wang, C. Tan, D. Yu1, “Provable datapossession of resource constrained mobile devices in cloudcomputing,” *Journal of Network*s **6 (7)** ,2011.

[9] Z. Zhou, D. Huang, “Efficient and secure data storage operations formobile cloud computing,” *IACR Cryptology ePrint Archive:* 185,2011.

[10] S.C. Hsueh, J.Y. Lin, M.Y. Lin, “Secure cloud storage forconventional data archive of smart phones,” *in: Proc. 15th IEEE Int. Symposium on Consumer Electronics, ISCE ’11*, 2011.

[11] W. Ren, L. Yu, R. Gao, F. Xiong, “Lightweight and compromiseresilient storage outsourcing with distributed secure accessibility inmobile cloud computing,” *Journal of Tsinghua Science and Technology***16 (5)** ,520–528,2011.

[12] Niroshinie Fernando, Seng W. Loke ,Wenny Rahayu, “Mobile cloudcomputing: A survey,” *Future Generation Computer Systems* **29 ,**84–106,2013.

[13] Ayesha Malik, Muhammad Mohsin Nazir, “Security Framework for Cloud Computing Environment: A Review,” *Journal of Emerging Trends in Computing and Information Sciences, 2012. DhammapalTayade / (IJCSIT) International Journal of Computer Science and Information Technologies*,**5 (5)** , 2014.

[14] Preeti Garg, Dr. Vineet Sharma , “Secure Data Storage in Mobilecloud computing” *Internatyional Journal of Scientific Research*,**4 (4)**,2013.

[15] K. Hwang, S Kulkarni and Y. Hu, “Cloud security with virtualized defence and Reputation-based Trust management,” *Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628, Chengdu*, 2009.