International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 09 | Sep 2018 www.irjet.net p-ISSN: 2395-0072

Securely P2P File Access Availability in Mobile Ad Hoc Networks though Replication for Efficient File Sharing

Rakhi Rajendra Burghate[1], Prachi Ghogare[2], Ashwini Ghotkule[3], Jyoti Jatade[4]

[1,2,3,4]*Department of Computer Engineering, JSPM Rajarshi Shahu College of Engineering Tathawade Pune Savitribai Phule Pune University, Maharashtra, India*

Abstract:- *File sharing applications in mobile ad hoc networks (MANETs) have attracted more and more attention in recent years. The efficiency of file querying suffers from the distinctive properties of such networks including node mobility and limited communication range and resource. An intuitive method to alleviate this problem is to create file replicas in the network. However, despite the efforts on file replication, no research has focused on the global optimal replica creation with minimum average querying delay. Specifically, current file replication protocols in mobile ad hoc networks have two shortcomings. First, they lack a rule to allocate limited resources to different files in order to minimize the average querying delay. Second, they simply consider storage as available resources for replicas, but neglect the fact that the file holders' frequency of meeting other nodes also plays an important role in determining file availability. Actually, a node that has a higher meeting frequency with others provides higher availability to its files. This becomes even more evident in sparsely distributed MANETs, in which nodes meet disruptively. In this paper, we introduce a new concept of resource for file replication, which considers both node storage and meeting frequency. We theoretically study the influence of resource allocation on the average querying delay and derive a resource allocation rule to minimize the average querying delay. We further propose a distributed file replication protocol to realize the proposed rule. Extensive trace-driven experiments with synthesized traces and real traces show that our protocol can achieve shorter average querying delay at a lower cost than current replication protocols.*

Key Words*: *Peer Connectivity, file sharing, file availability, mobile ad hoc networks (MANETs), P2P network

1. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a network consisting of a collection of nodes capable of communicating with each other without aid from a network infrastructure. Each node participating in the network works both as host and a router and must therefore is willing to forward packets for other nodes. For this purpose, a routing protocol is needed. The most important characteristics of MANET is the dynamic topology, nodes can change position dynamically therefore a need of a routing protocol that quickly adapts to topology changes. In this paper for experimental purpose, Investigators considered 150m x 150m, 250m x 250m, 350m x 350m, 450m x 450m, 550m x550m, 650m x 650m & 750m x 750m terrain area and illustrate the Drop packet analysis using DSR protocol parameters for wireless network scenario. The *Dynamic Source Routing* protocol, a simple as well as an efficient routing protocol is designed particularly for use in multi-hop wireless ad hoc networks, allows the network to be entirely self-organizing and self-configuring, without the requirement of any presented network infrastructure or the administration. All aspects of the protocol work entirely *on-demand*, permitting the routing packet overhead to scale *automatically* to only which needed to respond to various changes in the different routes currently in use.

2. PROBLEM STATEMENT

The Problem of the system is to define the fact that File replication is an effective method to deal with the problem of overload condition due to flash crowds or hot files. It distributes load over replica nodes and improves file query efficiency. File consistency maintenance to maintain the consistency between a file and its replicas is indispensable to file replication. Requiring that the replica nodes be reliably informed of all updates could be prohibitively costly in a large system.

3. LITERATURE SURVEY

3.1 ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks

In hostile environments, the enemy can launch traffic analysis against interceptable routing information embedded in routing messages and data packets. Allowing adversaries to trace network routes and infer the motion pattern of nodes at the end of those routes may pose a serious threat to covert operations. We propose ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks deployed in hostile environments. We address two closely related problems: For *route anonymity*, ANODR prevents strong adversaries from tracing a packet flow back to its source or destination; for *location privacy*, ANODR ensures that adversaries cannot discover the real identities of local transmitters. The design of ANODR is based on "*broadcast with trapdoor information*", a novel network security concept which includes features of two existing network and security mechanisms, namely "broadcast" and "trapdoor information". We use simulations and implementation to validate the effectiveness of our design.

3.2 An Efficient Anonymous Routing Protocol for Mobile Ad Hoc Networks

Providing anonymous routing in mobile ad hoc networks (MANET) has been a hot issue for the purpose of security and privacy concerns. But there are very few have been done about providing a valid method to detect malicious node and providing a trustworthy protection over whole network. In this paper, we introduce a localized trust management which can primarily remove malicious nodes, and propose an efficient anonymous routing protocol by node that participates in the protocol encrypts entire message with trust key and says Hello to its ancestor within expiration time. It makes malicious node can be detected and isolated from the network. In this way, a anonymous and secure route path can be established in a hostile environment. Meanwhile, it is able to efficiently against the Denial-of-Service (DoS) attack.

3.3 MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks

The shared wireless medium of mobile ad hoc networks facilitates passive, adversarial eavesdropping on data communications whereby adversaries can launch various devastating attacks on the target network. To thwart passive eavesdropping and the resulting attacks, we propose a novel anonymous on demand routing protocol, termed MASK, which can accomplish both MAC-layer and network-layer communications without disclosing real IDs of the participating nodes under a rather strong adversary model. MASK offers the anonymity of senders, receivers, and sender-receiver relationships in addition to node un local ability and un track ability and end-to-end flow un trace ability. It is also resistant to a wide range of attacks. Moreover, MASK preserves the high routing efficiency as compared to previous proposals. Detailed simulation studies have shown that MASK is highly effective and efficient.

3.4 Improvise P2P File Sharing for Routing Efficiency

Now a day's mobile computing is becoming more and more popular. The efficiency of file querying suffers from the properties of networks which include node mobility and limited communication range and resource. File sharing is one of the aspects which include peer to peer file sharing over MANET. Main advantages of P2P file sharing are files can be shared without base stations, overload on server can be avoided and it can exploit the otherwise wasted peer communication opportunities among mobile nodes. File replication which plays important role in enhancing file availability and reduce file querying delay. By creating replicas the probability of encountered requests can be improved. Random Way Point used for the normal MANET and Community-Based Mobility Model used for Disconnected MANETs. In RWP, nodes are moving with random speed to the randomly selected points, so the probability of meeting each node is similar for all the nodes Community-based mobility model used in some content dissemination or routing algorithms for disconnected MANETs. So both models contain idea of resource for file replication, which considers both node storage and meeting frequency.

4. RELATED WORK

4.1 From cluster databases to cloud storage: Providing transactional support on the cloud.

Over the past three decades, technology constraints (e.g., capacity of storage devices, communication networks bandwidth) and an ever-increasing set of user demands (e.g., information structures, data volumes) have driven the evolution of distributed databases. Since flat-file data repositories developed in the early eighties, there have been important advances in concurrency control algorithms, replication protocols, and transactions management.

However, modern concerns in data storage posed by Big Data and cloud computing—related to overcome the scalability and elasticity limitations of classic databases—are pushing practitioners to relax some important properties featured by transactions, which excludes several applications that are unable to fit in this strategy due to their intrinsic transactional nature. The purpose of this thesis is to address two important challenges still latent in distributed databases: (1) the scalability limitations of transactional databases and (2) providing transactional support on cloud-based storage repositories.

Analyzing the traditional concurrency control and replication techniques, used by classic databases to support transactions, is critical to identify the reasons that make these systems degrade their throughput when the number of nodes and/or amount of data rockets. Besides, this analysis is devoted to justify the design rationale behind cloud repositories in which transactions have been generally neglected. Furthermore, enabling applications which are strongly dependent on transactions to take advantage of the cloud storage paradigm is crucial for their adaptation to current data demands and business models.

4.2 Replication: A Technique for Scalability in Cloud Computing

Cloud computing is a technology which produces and consumes huge amount of data every day. This makes the cloud to store tons of applications. The demand for these resources is on the rise. Multi cloud environment is used to satisfy these demands. If multiple providers cooperatively work together, the availability of resource can be improved. The replication of data across multiple places in cloud has become an effective solution to achieve good performance in terms of load balancing, response time and availability. Replication of data is a good way to achieve reliability and improve performance in a distributed system.

The rising popularity of cloud computing is an alternative to classic information processing systems. This has increased the importance of its correct and continuous operation even in the presence of faulty components. Fault tolerance is a

major concern to guarantee availability and reliability of critical services as well as application execution. In order to minimize failure impact on the system and application xecution, failures should be anticipated and proactively handled.

5. EXISTING SYSTEM

- In the former, redundant replicas are easily created in the system, thereby wasting resources. In the latter, though redundant replicas are reduced by group based cooperation, neighbouring nodes may separate from each other due to node mobility, leading to large query delay.
- There are also some works addressing content caching in disconnected MANETs/ DTNs for efficient data retrieval or message routing. They basically cache data that are frequently queried on places that are visited frequently by mobile nodes. Both the two categories of replication methods fail to thoroughly consider that a node's mobility affects the availability of its files.
- Node mobility, limited communication range and resource, have rendered many difficulties in realizing such a P2P file sharing system.
- Broadcasting can quickly discover files, but it leads to the broadcast storm problem with high energy consumption.
- In spite of efforts, current file replication protocols lack a rule to allocate limited resources to files for replica creation in order to achieve the minimum average querying delay, i.e., global search efficiency optimization under limited resources.
- Lack of higher ability.

Today, we can see that all of the storage is not properly secure it. Means, it is easily available of social network site. Any attacker is easily crack password and accesses all of data.

6. PROPOSED SYSTEM

In this paper, we introduce a new concept of resource for file replication, which considers both node storage and node meeting ability. We theoretically study the influence of resource allocation on the average querying delay and derive an optimal file replication rule (OFRR) that allocates resources to each file based on its popularity and size. We then propose a file replication protocol based on the rule, which approximates the minimum global querying delay in a fully distributed manner. We propose a distributed file replication protocol that can approximately realize the optimal file replication rule with the two mobility models in a distributed manner. Our experiment and simulation results show the superior performance of the proposed protocol in comparison with other representative replication protocols. Higher availability and mapping respective node.

7. SYSTEM ARCHITECTURE

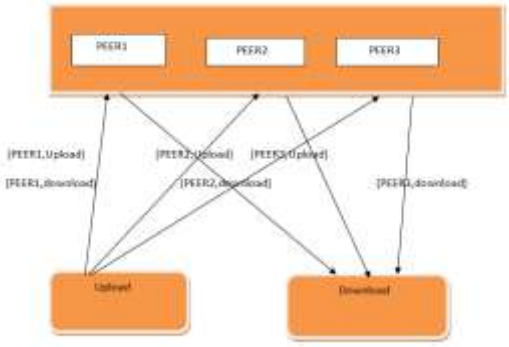


Fig -1 System Architecture

7.1 MODULE 1

File is sharing into IRM of equal size and k simultaneous connections are used. Client downloads a file from P2P at a time. Each peer sends a replication to the client.

7.2 MODULE 2

File is divided into many p2p and user downloads file replication sequentially one at time. The client randomly chooses the source peer at each time slot and download the file replication from each peer in the given time slots.

7.3 MODULE 3

Whenever a user completes a replication from its current source peer, the user randomly selects a new source peer and connects to it to retrieve a new p2p. Switching source peers based on chunk can reduce average time varying file download replications and updates.

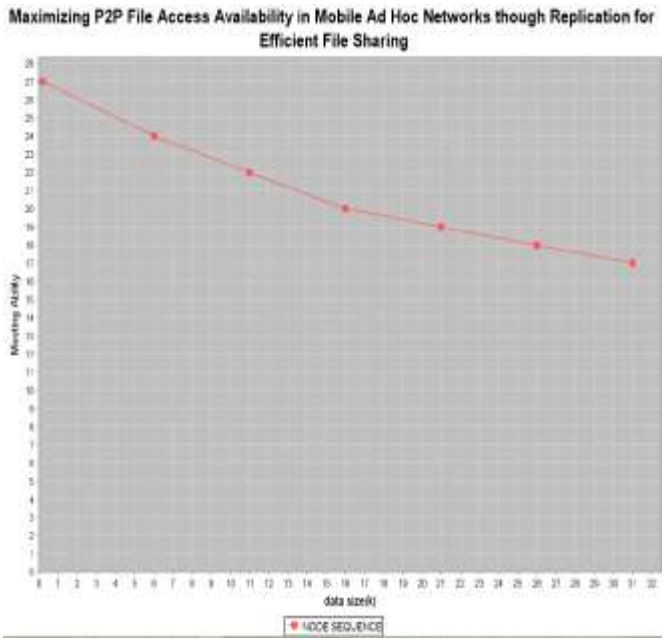
7.4 MODULE 4

File replication is an effective method to deal with the problem of overload condition due to flash crowds or hot files. It distributes load over replica nodes and improves file query efficiency. File consistency maintenance to maintain the consistency between a file and its replicas is indispensable to file replication. Requiring that the replica nodes be reliably informed of all updates could be prohibitively costly in a large system.

8. EXPERIMENTAL SETUP

In this the Structure consists of technologies like JAVA, HTML, CSS, Java script. For back end MySql is used. Hence before investigational set up Software like Eclipse, Tomcat is predictable to be installed on server. User must have basic windows Family, good browser to view the results. Supervised Dataset or Un-Supervised dataset is used for testing in MySQL is tested.

9. RESULT



Above graph create replica in sequence manner.

X-> data size

Y->Time in ms

10. ALGORITHM

1. START

2. Input le is F(z)

3. count =0;

4. create replica node is an n1(z)

5. count increased count+1;

6. set order list for replica

7. for each le F(z) node

while(R(Z) !=null)

n1 is an R(Z). createReplica() function for respective node

8. find F(z) node total memory

9. F(Z) =f1,f2,f3..... is a replica store randomly particular server respective le name

10. F(Z).Size()is performs reduce

11. Then download the merger le respective le name

12. nSum calculates with nTotal+nRandom+fn(z)

13. return nSum that is F(Z)

14. End.

11. CONCLUSION

We can conclude that how to put securely file on server. Also, File replication is an effective method to deal with the problem of overload condition due to flash crowds or hot files. It distributes load over replica nodes and improves file query efficiency. File consistency maintenance to maintain the consistency between a file and its replicas is indispensable to file replication. Requiring that the replica nodes be reliably informed of all updates could be prohibitively costly in a large system.

12. REFERENCES

[1] "Qik," http://qik.com/, 2014.

[2] "Flixwagon, " http://www.flixwagon.com/, 2014.

[3] Y. Tseng, S. Ni, and E. Shih, "Adaptive Approaches to Relieving Broadcast Storms in a Wireless Multihop Mobile Ad Hoc Network," Proc. 21st Int'l Conf. Distributed Computing Systems (ICDCS), pp. 481-488, 2001.

[4] B. Chiara et al., "HiBOp: A History Based Routing Protocol for Opportunistic Networks," Proc. IEEE Int'l Symp. World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2007.

[5] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in Intermittently Connected Networks," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 7, no. 3, pp. 19-20, 2003.

[6] F. Li and J. Wu, "MOPS: Providing Content-Based Service in Disruption-Tolerant Networks," Proc. IEEE 29th Int'l Conf. Distributed Computing Systems (ICDCS), 2009.

[7] S. Moussaoui, M. Guerroumi, and N. Badache, "Data Replication in Mobile Ad Hoc Networks," Proc. Second Int'l Conf. Mobile Ad-hoc and Sensor Networks (MSN), pp. 685-697, 2006.

[8] L. Yin and G. Cao, "Supporting Cooperative Caching in Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 1, pp. 77-89,Jan. 2006.

[9] T. Hara and S.K. Madria, "Data Replication for Improving Data Accessibility in Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1515-1532, Nov. 2006.