

DETECTING DORMANT AND MALICIOUS TRANSMISSION NODES IN FAULT TOLERANT CLOUD COMPUTING ENVIRONMENT

J.UDAYA KUMAR, (Asst.Professor),
Dept.of CSE, P.K.I.E.T, Karaikal.
Email:uday.ja@gmail.com

V.HARIPRIYA,
Dept.of CSE, P.K.I.E.T, Karaikal.
Email:haripriya330@gmail.com.

K.VEMBOU,
Dept.of CSE, P.K.I.E.T, Karaikal.
Email:haripriya330@gmail.com.

S.SELVASEKARAN
Dept.of CSE, P.K.I.E.T, Karaikal.
Email: sbk1323@gmail.com

VajraNaga Vikas.T
Dept.of CSE, P.K.I.E.T, Karaikal.
Email: vikky.nani223@gmail.com.

Abstract— As the increase in the computing resources exceeds the computing performance the distributed system or develop and used to overcome these disadvantages. It is necessary to overcome the fault situation occurring during the access of multiple resources in cloud computing environment. These distributed systems always follow a certain agreement protocol to recover from unwanted deadlock situation. Dual agreement protocol achieves this, by transferring minimum number of messages among all the nodes. The dormant or faulty transmission node is always problem in the dual agreement protocol. In this project, we propose a modified fault tolerance algorithm to detect dormant and to locate malicious transmission in the distributed systems. In a cloud-computing environment, the connected topology is not very significant. Therefore, previous protocols for the agreement problem are not suitable for a cloud-computing environment. To enhance fault-tolerance, the agreement problem in a cloud-computing environment is revisited in this study. The proposed protocol is called the Dual Agreement Protocol of Cloud-Computing (DAPCC). DAPCC achieves agreement on a common value among all nodes in a minimal number of message exchange rounds, and can tolerate a maximal number of allowable faulty components in a cloud-computing environment.

1. INTRODUCTION

Cloud-computing efficiently support user-oriented service application. However, distributed systems have grown rapidly in both size and number. In a distributed computing system, nodes allocated to different places or in separate units are connected together so that they collectively may be used to greater advantage. In many cases, reaching a common agreement in the presence of faulty components is the central issue of fault-tolerant distributed computing, because many applications require such agreement. Some examples of such tasks include clock synchronization and locating a replicated file in a distributed system. Currently, cloud-computing can ensure increased ability to use the low-power nodes to achieve high reliability. Furthermore, many applications of cloud-computing increase convenience for users. For users, the system must provide better reliability and fluency. Therefore, node reliability is one of the most important aspects of cloud-computing. To ensure that a cloud-computing environment is reliable, a mechanism to allow a set of nodes to reach an agreed value is necessary. The Byzantine Agreement (BA) problem is one of the most fundamental problems concerning reaching agreement in distributed systems. It is a well-known paradigm for achieving reliability in a distributed network of nodes. According to the definition of the BA problem there are

n nodes, of which at most $b(n-1)/3$ nodes could fail without breaking down a workable network. The nodes communicate with each other through message exchange in a fully connected network. The message sender is always identifiable by the receiver; and a node is chosen as a source, and its initial value v_s is broadcasted to other nodes and itself to execute the protocol [1].

2. PROBLEM DEFINITION

MOTIVATION:

In a cloud-computing environment, the connected topology is not very significant. Therefore, previous protocols for the agreement problem are not suitable for a cloud-computing environment. To enhance fault-tolerance, the agreement problem in a cloud-computing environment is revisited in this study. The proposed protocol is called the Dual Agreement Protocol of Cloud-Computing (DAPCC). DAPCC achieves agreement on a common value among all nodes in a minimal number of message exchange rounds, and can tolerate a maximal number of allowable faulty components in a cloud-

computing environment.

PROBLEM DEFINITION:

These distributed systems always follow a certain agreement protocol to recover from unwanted deadlock situation. Dual agreement protocol achieves this, by transferring minimum number of messages among all the nodes. The dormant or faulty transmission node is always problem in the dual agreement protocol. In this project, we propose a modified fault tolerance algorithm to detect dormant and to locate malicious transmission in the distributed systems [4].

3. RELATED WORK

The problem is to make the correct nodes in an n -node distributed system reach interactive consistency. Each node chooses an initial value and communications with the others by exchanging messages. There is interactive consistency in that each node i has its initial value v_i and agrees on a set of common values. Therefore, interactive consistency has been achieved if the following conditions are met: Agreement: Each correct node agrees on a set of common values.

The traditional agreement problem focused on a Fully Connected Network (FCN), a Broadcasting Network (BCN) or a Generalized Connected Network (GCN). However, cloud-computing is an Internet-based development. It is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Nevertheless, in a cloud computing environment,

the connected topology is not very significant. Therefore, previous protocols of the agreement problem are not suitable for a cloud-computing environment [7].

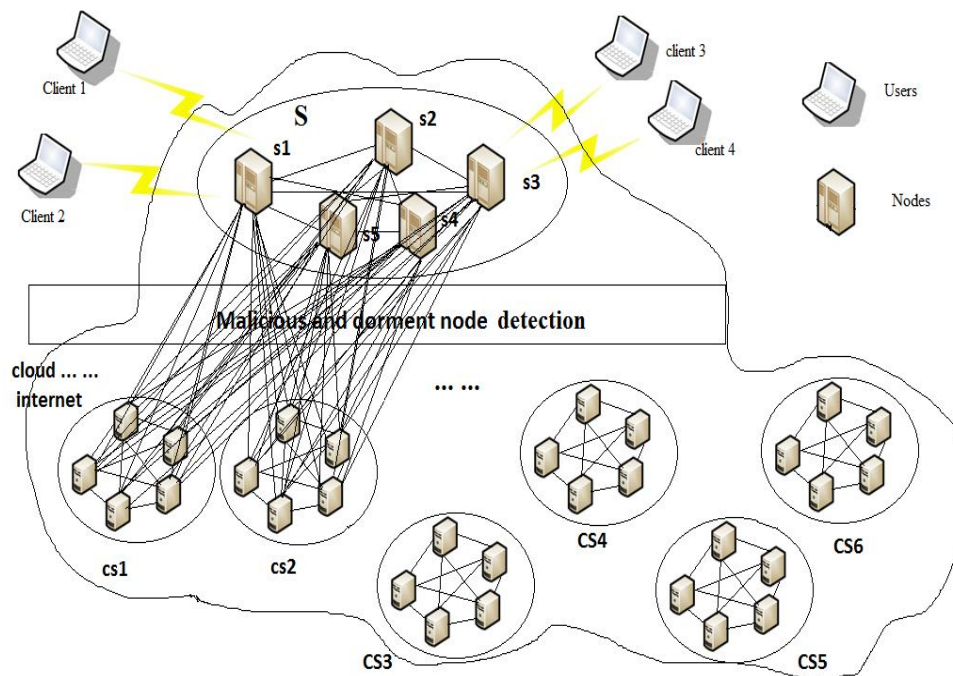
4. EXISTING WORK

In the previous literature, the agreement problem has been solved in a Fully Connected Network (FCN), a Broadcasting Network (BCN) or a Generalized Connected Network (GCN). With the advancement and development of various technologies, computing problems become more complicated and larger. A cloud-computing environment allows a user faster operation of Internet applications. The majority of cloud-computing [3].

5. FUTURE WORK:

In this project the Dual Agreement Protocol is implemented in the cloud computing environment with the detection of Dormant and Malicious nodes. The proposed protocol DAPCC is improved and it contains two parts Interaction process and Agreement process. In the interaction process the nodes in the first layer collect the user request and send these request to the second layer to satisfy the request the node in the first layer interacts among themselves. A timer is used to detect the dormant nodes in the group. When a particular

node remains idle without communicating with each other for specified amount of time. It is detected as a dormant node and is communicated to other nodes in group [4].



Example of topology of Cloud-computing

6. CONCLUSION

Finally to conclude this paper, As the increase in the computing resources exceeds the computing performance the distributed system or develop and used to overcome these disadvantages. It is necessary to overcome the fault situation occurring during the access of multiple resources in cloud computing environment. This protocol can use a minimal number of rounds of message exchange and tolerate a maximal number of allowable faulty nodes in a cloud-computing environment. The agreement problem for dormant or malicious faulty nodes in cloud-computing environment is revisited and the fault-tolerance capacity is enhanced by DAPCC. Dual agreement protocol achieves this, by transferring minimum number of messages among all the nodes. The dormant or faulty transmission node is always problem in the dual agreement protocol. In this project, we propose a modified fault tolerance algorithm to detect dormant and to locate malicious transmission in the distributed systems [1].

7. REFERENCE

- [1] Aymerich, F. M., Fenu, G., & Surcis, S. (2008). An approach to a cloud computing network. In The proceedings of first international conference on the applications of digital information and web technologies, Czech Republic (pp. 113–118).
- [2] Barborak, M., Malek, M., & Dahbura, A. (1993). The consensus problem in fault tolerant computing. *ACM Computing Surveys*, 25(2), 171–220.
- [3] Bar-Noy, A., Dolev, D., Dwork, C., & Strong, R. (1987). Shifting gears: Changing algorithms on the fly to expedite Byzantine agreement. In The proceedings of the 6th annual ACM symposium on principles of distributed computing, Vancouver, British Columbia, Canada (pp. 42–51).
- [4] Cheng, C. F., Wang, S. C., & Liang, T. (2009). The anatomy study of server-initial agreement for general hierarchy wired/wireless networks. *Computer Standards & Interfaces*, 31(1), 219–226.
- [5] Fischer, M. (1983). The consensus problem in unreliable distributed systems (a brief survey). In The proceedings of the 1983 international fault tolerance computer conference. Lecture notes in computer science, Borgholm, Sweden (pp. 127–140).
- [6] Gifford, D. K. (1979). Weighted voting for replicated data. In The proceedings of the seventh ACM symposium on operating systems principles, Pacific Grove, California, United States (pp. 150–162).
- [7] Grossman, R. L., Gu, Y., Sabala, M., & Zhang, W. (2009). Compute and storage clouds using wide area high performance networks. *Future Generation Computer Systems*, 25(2), 179–183.
- [8] Halsall, F. (1995). *Data links, computer networks and open systems* (4th ed.). Addison-Wesley Publishers Ltd.
- [9] Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine general problem. *ACM Transactions on Programming Language and Systems*, 4(3), 382–401.
- [10] Meyer, F. J., & Pradhan, D. K. (1991). Consensus with dual failure modes. *IEEE Transactions on Parallel and Distributed Systems*, 2(2), 214–222.
- [11] Molina, G. (1986). Application of Byzantine agreement in database system. *ACM Transactions on Database Systems*, 11(1), 24–47.
- [12] Pease, M., Shostak, R., & Lamport, L. (1980). Reaching agreement in presence of faults. *Journal of ACM*, 27(2), 228–234.
- [13] Pei, G., Gerla, M., Hong, X., & Chiang, C. C. (1999). A wireless hierarchical routing protocol with group mobility. In The proceedings of IEEE wireless communications and networking conference, Los Angeles, California, United States (pp. 1538–1524).