ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

System Intelligent Agent in Distributed Computing

Prof.B.Murali[1], Ms.A.Mary Subasree[2]

Associate Professor & Head, Department of Computer Science, PSG College of Arts & Science, Coimbatore, India [1]

M.Phil. Research Scholar, Department of Computer Science, PSG College of Arts & Science, Coimbatore, India [2]

Abstract: The Internet is a global network connecting millions of computers. The Industries based on network and information sharing is wide spread across the world having major control on the economic sector of the world. Networking and distributed computing plays the key role for the survival of IT industries. The downtime in these sectors caused by the failure in the distributed networks is handled by various techniques. Network management agents have existed for years; System agents are one such software agents whose main job is to manage the operations of a data communications network. These agents monitor for device failures or system overloads and redirects work to other parts in order to maintain a level of performance and reliability. This paper surveys various agent techniques that reduce down time caused by system failure and states the effects of the system down time and the use of system agent in the field of distributed computing is analysed.

Keywords: Distributed computing, downtime in IT, fault tolerant agents, system agents.

I. INTRODUCTION

The Internet is more of a concept than an actual tangible entity, and it relies on a physical infrastructure that connects networks to other networks. No one owns Internet, although several organizations in the world over collaborate in its functioning and development. The information technology (IT) industry has become one of the most robust industries in the world. The entire process in an IT industry depends on the distributed systems that are built based on the networks.

Distributed computing deals with the study of the distributed systems that forms a large clustered or group of networks. Distributed system is a software system in which components located on networked computers communicate and coordinate their actions by passing messages. There are various complexities in the distributed systems so that the system should be fault tolerant in order to communicate. So, failure or an outage brings a huge damage in this IT industry. There are various reasons that causes down time in the IT industries, but a major role is played by failure of the networks. Agents are the intelligent software which can act without human interference. Agent technologies are used to simplify the complexities in the field of distributed computing as an agent such as system agent can able to perform functions such as

- Manage the operations of computing system
- Monitor for failure of devices
- Monitor system overloads
- Redirect the work to all the parts

Many novel fault tolerant mechanisms are provided in [1] with features such as minimizing the node failure, fast identification of the failed nodes, execution and consistent working of the failure networks and communication for mobile agents based distributed systems.

II. DOWN TIME IN IT INDUSTRIES

A. What is down time?

The term downtime or outage duration refers to a period of time that a system fails to provide or perform its primary function. The unavailability is the proportion of a time-span that a system is unavailable or offline. This is usually a result of the system failing to function because of an unplanned event, or because of routine maintenance. The term is commonly applied to networks and servers. The common reasons for unplanned outages are system failures or communication failures.

B. Reasons and effects of system down time

The There are various reasons that cause the system to go unavailable, important reason regarding the system down time in IT industries are failures in the network, failure of hardware or software, over load in the network, bad network cable, failure in routers, failure of the mobile agent. On average, businesses lose between $84,000 and $ 108,000 (US) for every hour of IT system downtime, according to estimate from studies and surveys performed by IT industry analyst firms. In addition financial services, telecommunications, manufacturing and energy lead the list of industries with a high rate of revenue loss during IT down time. The effect caused by the above mentioned reasons are loss of revenue, reputation, productivity which results in a great fall on the sector of the world.

III. VARIOUS FAULT TOLERANT TECHNIQUES AND APPROACHES

The term fault tolerant specifies the ability of the system to respond to any unexpected failure. Its main goal is to establish a reliable functioning of the agent even at the time of failure. The fault tolerant technique used in the traditional distributed architectures is often static, require special infra-structure support and restricts the

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

functionalities of the agent frame works [2]. The system down time is reduced with the help of various fault tolerant agents. These fault tolerant techniques in agent systems are mainly based on temporal and spatial approaches. In [3] authors discussed many fault tolerant approaches using CAMA(Context aware mobile agent) Framework, optimistic replication approach, region based protocol construction, using witness agents. Few of the fault tolerant techniques for agents are discussed in Table I.

TABLE I: Fault tolerant mechanism

Techniques	**Approaches for fault tolerance**
CAMA Framework	Exception handling
Optimistic replication	Check pointing, chain control and message passing
Fault tolerant mobile agent system	Agent dependent: logger agent-check pointing, logging
Witness agent in 2D mesh network	Cooperation of agents
Transient fault tolerance	Comparing image codes using XOR algorithm

Fault tolerant techniques and approaches

A. CAMA Framework

The Context Aware Mobile Agent framework provides fault tolerance in application level with middle ware technologies that features indicating error detection and recovery. It supports fast and effective exception handling mechanism with major operations such as raise, wait and check.

B. Title and Author Details

Optimistic Replication approach supports agent to avoid blocks in the networks and focuses on the transactional execution and semantic failures. It is based on many transactional protocols for communication between the agents in the network. It uses check pointing, chain control and message passing.

C. Witness Agents in Mesh Network

Agents are cooperated in this technique so that server and agent failures are easily detected and recovered. It monitors for the lively hood of the agents in the networks. Agents used in this techniques performs program for owners (actual agent), monitors the actual agent (witness agent), sent for recovery of agents (probe).Communication among the agents is done by messaging passing.

IV. SYSTEM AGENT USING SNMP

An agent is a computational system, situated in some environment that is capable of intelligent, autonomous action in order to meet its design objectives. Its notable characteristics are mobility, proxy, reactive, autonomous and decision making.

A. How does system agents work at down time?

The system agent as mentioned serves as software that detects the node failure and monitors the nodes in the distributed network. This agent prevents and reduces the losses by system down time effect caused due to network failure within minimum time. System agent also communicates with other agents in the system to get the information about the failure nodes in the network. As computer installation becomes more distributed the need for system agents arises. An intelligent agent that processes information collected by SNMP agents and uses it to detect anomalies that typically precede a fault as proposed in [4].

B. Role of SNMP Agent

SNMP is the protocol used to communicate network management information between nodes on a network running on the IP protocol. SNMP serves as a best example for the system agent working in the network. The information gathered from each node must also be in a standard format, so that [5]:

Including the network manager knows what pieces of information can be retrieved.
The information provided through SNMP is understandable to the software making the request.

This standard format is provided by the Management Information Base (MIB) standard specification. MIBs are a collection of definitions which define the properties of managed object within the device to be managed such as router, switch, etc. Each managed device keeps a database of values for each of the definitions written in the MIB. The MIB database contains the object identifier (OID) information. The OID identifies the individual entries in the MIB.

V. PROBLEM DESCRIPTION AND SOLUTION

The SNMP manager communicates by sending SNMP messages that contains information request for the number of active sessions, name of the community and the destination of the message through the SNMP service libraries. On receiving the message the host checks the community name in the packet and evaluates the request and verifies the IP address of the source. If all the verified information is valid then the request is accepted but if the community name is incorrect then agent sends authentication failure trap to the particular trap destination. But when a problem occurs during the communication between the SNMP manager and the agent in the network, it results in failure of network and also a cut in the connection appears. One such major problem is node failure. If the node where the agent resides fails it will affect the entire network. So, a solution to this problem is stated with Bayesian network and Distributed Cut Detection algorithm. The node information is mined and knowledge about the failure is obtained.

A. Network Construction

In Bayesian network consists of a set of variables and directed edges between variables (nodes), and each variable has finite set of mutually exclusive states,

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

together with the edges forms a directed acyclic graph. Steps to construct the algorithm follow:

- Choose a set of nodes that describes the application domain.
- Choose an ordering of nodes i.e., S1 . . . SN.
- Start with the empty network and add nodes to the network in DSN environment.

  For i = 1 to N
  Add Si to network
  Select parents from S1 . . . SN such as
  P (Si | parents (Si)) = P (Si | Si..Si−1)
  Next i
- Draw an arc from the each node in parents (Si) to Si.

B. Failure Node Detection

To avoid and detect the node failure problem a Distributed Cut Detection algorithm is used. The algorithm consists of nodes, updating their local state periodically by communicating with their nearest neighbors. The state of a node converges to a positive value in the absence of a cut. If a node is disconnected from the source as a result of a cut, its state converges to 0 (deactive). The state of node determines whether it is connected to source or not. One of the nodes of the network is a specially designed node which is always active called as "source node". Let G = (V, E) denote the undirected sensor network that consists of all the nodes and edges of G that are active at time k, where k = 0, 1, 2.. is an repetitive counter. If no cut occurs or else no node fails then state of every node converges to a positive number. If a cut occurs at a time T > 0 which separates the graph G into N connected components Gs,., GN, where the component Gs (Vs., Es) contains the source node, then

(1) State of every node disconnected from the source node converges to 0 (deactive) and

(2) State of every node in Vs converges to a positive number.

C. Results Obtained

In the Bayesian Network, nodes represent the variables and arcs indicate probabilistic dependencies between nodes. Inferences are used in the process of deriving a logical conclusion. Inference is used to compute the conditional probability for nodes with given information (evidence) concerning other nodes or variables.It maintains the update message function. It consists of node ID, energy, bandwidth and link efficiency. Based on the update message function, source node calculates the probabilities of each node. The tables provide the results calculated with probability values with the parameters such as distance, link efficiency and energy. Data is sent from the source to a particular node and the node information is obtained from the management information base.

The tables II and III predicted results states the probability of the node failure with the value change in energy, distance and link efficiency.

TABLE II : Distance with Link efficiency

Distance/Link efficiency	**Low**	**Fair**	**High**
Minimum	0.55	0.78	0.93
Fair	0.51	0.73	0.86
Maximum	0.43	0.69	0.79

Frequent analysis of parameters

TABLE III : Predicted Results

Energy	**Distance**	**Link efficiency**	**Result**
Maximum	High	Minimum	High
Maximum	Fair	Minimum	Fair
Minimum	High	Minimum	Minimum
Fair	High	Minimum	High
Maximum	Minimum	Fair	Fair
Maximum	Minimum	Maximum	Minimum

Frequent analysis of parameters with results

VI. CONCLUSION

In this paper the effects of the downtime in IT industries due to the system or network failure is discussed. Many fault tolerant approaches are used in the agents to prevent the failure in the network and the approaches use different methodologies to keep fault free systems in the distributed network. Through the use of SNMP system agents, the information technology system monitoring has grown dramatically and has drastically reduced the requirement for administrators to manually monitor individual network components. The solution provided to the node failure problem and predicted results can also be further enhanced by including the prediction of other parameter values. Thus it helps in a better way to reduce the down time effects caused by the node failure that occur in the distributed systems.

REFERENCES

[1] Jinho Ahn, "Fault-tolerant Mobile Agent-based Monitoring Mechanism for Highly Dynamic Distributed Networks",IJCSI International Journal of Computer Science Issues, Vol. VII, pp.443-760, May 2010.

[2] S.Kumar, P.R.Cohen, "Towards fault tolerant multi agent system architecture" In proceedings of the fourth international conference on Autonomous Agents,pp. 459-466,2000

[3] Richa Mahajan,Gurpreet Singh,Ramandeep Kaur and Rahul Han " Comparative Analysis of Various Fault Tolerance Approaches in Mobile Agents System" vol IV, International Journal of Information and Computation Technology, ISSN 0974-2239,pp.343- 350,2014

[4] C.S.Hood, C.Ji, "Intelligent Agents for Proactive Fault Detection" , IEEE Internet Computing, vol.2, no.2, pp.65-72, Mar/Apr 1998.

[5] Peter Murray and Paul Stalvig "White Paper-SNMP Simplified 03/08",F5 networks Inc.ltd,2008