Abstract—Mobile agent technology is new in the area of distributed computing today. The mobile applications are widely used today because of their easy accessibility. The agents can easily migrate from network to network and can sense environment and act accordingly. They don’t need any external interfaces to act with. The tasks can quickly and easily be accomplished as they cooperate and coordinate with other agents. However, besides various applications offered by mobile agents due to their mobility, they too suffer from faults and security issues. Fault tolerance is the ability to provide responses to unexpected failure in a graceful manner. Also various security risks have been encountered associated with mobile applications. Assessing the possible risks and vulnerabilities for the system is very important today in order to protect the mobile applications. The paper discusses the appropriate approaches and strategies that need to be adopted to resolve difficulties in area of mobile applications.

Index Terms—Communication, Digital Libraries, Library, Library Professionals, Technology.

I. INTRODUCTION

A new paradigm in the area of mobile and distributed computing is mobile agent technology. Due to the various issues regarding reliable mechanism such as fault tolerance and security, the mobile agents are not widely used. Mobile agents suffer from various faults due to their mobility. Due to faults, mobile agents may be unable to perform and continue their executions as the failure of any component or link can occur at any time.

Fault tolerance is the ability to provide responses to unexpected failure in a graceful manner. Some of the common failures that mobile agents face while migrating from network to network are message loss, node failure, communication failure, component fault etc. Also, security is one of the major issues in case of mobile agents. Denial of service is a common attack commonly known as black hole attack where the packets are purposely dropped by finding a shortest path to the destination node. Various security risks have been encountered associated with the mobile applications.

The goals of information security that are confidentiality, integrity and availability can be severely harmed if the risks are not analyzed to the depth. Assessing the possible risks and vulnerabilities for the system are very important today. Strict countermeasures are required to be applied in order to protect the mobile applications. Ethical approaches needs to be used while designing the applications in order to protect the applications in order to protect them from exploitation. The protection levels and permissions should be studied in detailed manner. The analyst must be open to accept both that is there is a need to consider a single remedial action that can reduce a sum of multiple risks whereas intersection of multiple remedial actions to counter a security issue in an organization.

The attacks to network hinder the performance by reducing the packet delivery ratio. Though there are various efficient algorithms that provide various benefits such as supports multi-hop routing, dynamic, loop free and automatically detects inactive routes but they are not at all secure. The vulnerabilities to network are still there. The algorithms need to be modified in an appropriate manner in order to encounter the security issues. The performance of the network parameters such as routing overhead, end to end delay, throughput, packet delivery ratio need to be compared.
in all the scenarios. Innovative approaches and strategies need to be adopted in order to secure mobility.

II. LITERATURE REVIEW

Today there is quite a quick growth in the market of mobile applications and also in demand of user towards them. The development of software for portable handheld devices is the core process of mobile application development. The mobile application with suitable requirements, characteristics and capabilities are adopted to be developed by teams working on software projects in order to face the demand that is ongoing today in the market. The development of mobile applications focuses on development and growth in a continuous manner tailored towards meeting the needs of clients. However an increasing demand of mobile applications has been experienced with the advancement of communication technologies and mobile computing.

Mobile applications today are also facing various challenges. One of the big challenges are the changes in user requirement on regular basis. The systems become more complex due to the frequent changes in customer expectations and modifications. Secondly in order to maintain the service quality and its continuity a mobile user has to switch between networks. This also poses a challenge to mobility as one has to deal with multiple technologies being accessed. Network architecture is also a major challenge as the mobile clients are dependent on dissimilar networks integrated wirelessly for accessing the services. Moreover quality of service and requirements of the most economical services are on the demands of mobile users.

In order to continue the mobile service as a mobile user roam across different areas and during that session a number of service providers will be involved various schemes of charging may be used. This has also encountered as a challenge today being an important factor for efficiency. Vulnerability of mobile services is still there because of internetworking and interconnected networks. The paper tends to work out by providing innovative practices towards facing all the various above mentioned challenges and overcoming the security issues in mobile computing. The approaches and strategies illustrated helps in facing the problems of mobility today that are being faced by mobile clients and provides fault tolerance to mobile users in an efficient manner.

III. APPROACHES TOWARDS FAULT TOLERANCE IN MOBILE AGENT SYSTEMS

The ability of mobile agents to move from one network to another provides it with characteristics that differentiate it from other paradigms. Faults may occur at any time in mobile agents due to the failure of any link or component. A graceful respond to these failures is termed as fault tolerance. Some of the approaches towards fault tolerance are as follows:-

A. Exception Handling Approach:- By allowing designers to design recovery mechanism and error detection CAMA framework can provide a supporting middleware and a set of abstractions supporting fault tolerance at application level. Exception Handling provides recovery to the application in a fast manner. However the drawback of this approach is that the execution gets blocked once an agent encounters an exception.

B. Check Pointing Approach:- Avoid situation of blocking thereby allowing mobile agent to execute at multiple times. It makes use of message passing approach. Lookup directories are used for detecting multiple executions. They are solved as only one execution is committed at the destination place. The approach provides benefit as the property of committing at the destination place and that also only once is not at all violated using it. However, partition of network could not be tolerated using this approach and the detection of failure could not be assumed perfectly.

C. Replication Based Fault Tolerance Protocols:- The agent is sent to various sites after it is replicated in case of spatial replication. An extra communication cost is added which is the drawback of this type of replication. In case of multi region computing environment region based protocol is used in which quasi participant concept is used in order to put together some places located in different regions within a stage in the same region. The total execution time is reduced which is the main benefit of this approach.

D. Agent Dependent Approach:- There is no need to modify the underlying platform thereby allowing fault tolerant execution of mobile agent. It uses the concept of logging and check pointing. An agent pair comprises of logger agent and user agent. Both the agents monitor each other and can use the local information in order to rebuild other if a fault is detected by one of them.

E. Non Periodic Fault Tolerance:- Many times the execution of mobile agents results in either complete or partial loss due to irregular or non periodic bit errors. Errors can be recovered by applying XOR computations on code images (original code and two replicas). In cases , the code is reloaded from stable
memory if the damage of all the three agent images have been encountered. The performance is increased through this approach as fault tolerance is applied at low level.

F. Usage of Monitoring Agent:- Another type of agents called as monitoring agents are used to detect whether the actual agent is alive or dead. This approach benefits by reducing complexity. However, lot of resources is consumed.

G. Implementation of RFID:- Various operations and reports can be controlled and managed using RFID technology. This technology work towards providing security to mobile agents as the tags are tracked and automatically identified attached to objects. Using this check-ins and check-outs of mobile agents can be done in a fast manner.

H. Designing Applications with Code Signings: - There is a need to design the mobile devices in such a ethical way that the user is prevented from getting exploited. The operating system should consist of password and identity for every application that runs on it. There should be the requirement to sign the application before it is executed. The protection level should be categorized as permission created by self during the process of development. The four levels can be:-

IV. MOBILE TECHNOLOGY APPLICATIONS
Being a technology that is new, applications that are distributed inherit several advantages. Some of the advantages are as follows:-

1. Saves the bandwidth usage:- A large amount of bandwidth is utilized during processing of data. Suppose as an example that a particular information is stored in a database that is centralized. A client server approach that is being traditional is shown in figure below. The desired information is retrieved from the server every time and is sent to the client that requested for that information. This process consumes a large amount of bandwidth.

Fig1: Data Processing before Mobile Technology

The approach of mobility is quite different which benefits the user by saving the bandwidth. In this approach an agent is sent itself to the server where the processing is done and all the information requested is sent back to the client. In case, a wide amount of information is desired, then this approach of using a mobile agent in a significant and beneficial manner, saves the bandwidth. This is as shown in figure below.

V. GRANTING PERMISSION AND SECURITY MECHANISM FOR MOBILE AGENTS
In order with a mobile system to interact with, it should be necessary to seek permission. A mobile application needs to take permission from a process built into the system known as validation process for completion of execution. For this, the API in mobile operating system such as Android commonly used undergoes three steps to make a call. They are:-

1. The API library is called.
2. Private Proxy Interface is then invoked by the library.
The service being executed in mobile system is then queried by the interface in order to seek permission to perform the operation. In order for a mobile system to be secure, there should be option to create and use permissions created by self. These permissions are declared commonly in .xml files. Also, one of the most common DOS attack known as black hole attack is encountered in mobile agent where the packets are dropped to the destination node through finding the shortest path. The system prevents the attack through maintaining software where the information about all the packets to be received gets stored in the database with their sending and receiving time. Now, when the packet is received the receiving time is checked and if the time is not valid the path can be rejected. Thus, in this way the information about packets can be counterchecked and the dropping of packets through shortest path is avoided. Easy access and administration is possible through a centralized database. The value of threshold can also be used for detecting and preventing black hole attack. In this two extra functions are added that is source node use threshold value to verify RREP from neighbor nodes and destination node use the defined threshold to verify the RREQ messages from source node. If the destination sequence number of RREP is greater than the threshold, it is considered as malicious node. Destination node also uses threshold value to identify the destination sequence number.

VI. CONCLUSION

Today mobile systems are widely used around the globe. However due to faults, mobile agents may be unable to perform and continue their execution as the failure of any component or link can occur at any time. Also accessing the possible risks and vulnerabilities are very important in order to protect the mobile applications from exploitation. There is a need to study the protection levels and permissions in a detailed manner to find the measures in order to deal with the issues of mobile applications in an appropriate manner. The paper provides us with various strategies and approaches that work towards handling the mobile agents in such a way that network parameters like routing overhead, end to end delay, throughput, and packet delivery ratio are improved and serves the end users in an efficient way.

VII. REFERENCES


Author Profile

Sangeeta Lalwani received the B.Tech degree from Moradabad Institute of Technology, Moradabad and M.Tech degree from Amity School of Engineering and Technology, Amity University, Uttar Pradesh, Noida, India in Computer Science and Engineering. Her areas of interest are Cloud Computing, Java Programming.

Anupam Bhardwaj received the BCA degree from Invertis University, Bareilly and M.Tech-M.CA dual degree from LPU, Punjab. His areas of interest are Cloud Computing, Java Programming, Networking, Software Engineering.