CHAPTER ONE : INTRODUCTION

In this chapter, an introduction to the accomplished research is presented. First, a general idea of self-regenerative system as a background of this research is given. Afterward an overview of problem that we address in our research as well as question needed to be answered; furthermore objective of this research is discussed. We also the contribution and research structure is stated. Finally a methodology of this research and scope is discussed.

1.1 Introduction

The modern computer network world is a complex combination of different components, with the purpose of making recourses or software available to those who need it. Unfortunately, access to the networks by unauthorized users and threats are growing at a rate that far outpaces any thing we could have imagined (Thomas et al, 2005), which makes software unsaved and vulnerable. Lots of actions needed for developing mechanisms and protocols to meet the security expected. In recent years many effort have been made in developing algorithm and methodology, for building efficient network security mechanism using self-regeneration.

A self-regenerative system can be defined as a system that implements a set of capabilities enabling it to recover from attacks as well as to restore its functionality while removing exploit vulnerabilities (Saidi et al, 2003). This knowledge aims to develop technologies enabling systems to learn, regenerate themselves, and automatically improve their ability to deliver critical services. If successful, self-regenerative systems will show a positive way in reliability, in fact it exceeds initial operating capability and approaching to a theoretical existence of system over time. Self-regeneration capabilities are ways of securing nodes that is particularly being affected by malicious attacks. These actions meant to respond automatically to both accidental faults as well as improve overall security (Palul et al, 2005). We seek to address these deficiencies by creating

security mechanism and survivability technique. This technique goes to save network component software from failure, which is biologically inspired.

Currently, technology is moving toward a more sufficient capability in securing component or software in a node form failure, which is Autonomic Computing. Autonomic Computing is a technological realization of the disposition of natural biological systems toward maintaining systemic equilibrium conditions through integrated feedback mechanisms, beside, the concept of self-management and adaptation in computing systems has been around for some time (McCann et al, 2004). Several autonomic activities or biologically inspired mechanism can be extracted from nature.

Biologically inspired systems are the capabilities that is extracted form nature, this biologically inspired technology have made a fast development and significant in recent years. More mechanism of biological phenomena becomes an approach for researchers in so many areas particularly network security realm (Wei et al, 2006). We support our research using the cell biochemical reaction and cell regeneration such as organic molecule production from DNA.

Furthermore, in most cases today, a distributed computing architecture consists of very lightweight software components distributed on a number of client systems (Nodes), and one or more dedicated distributed computing management servers. Theses component communicates from each other in order to deliver a services. Attacks to the components can be critical issue to the availability. Therefore, the need at this point is the reliability of the component in distributed environment.

1.2 Problem identification

In a distributed system, components are vulnerable and can fail to respond due to failure or attacks, the consequence of failure could cause damage to the whole system. Therefore, survivability and robustness is needed to maintain the availability of the

system overtime. Consequently, we have to identify solutions considering certain cases where the failure of the system is crucial.

1.3 Research Questions

Based on the identification of the problem above, how can we avoid failure in distributed component based software, and can the attack be detected before damage and then regenerate components. Furthermore, Can a mechanism be built to perform a proactive and reactive action if the system faces attacks?

1.4 Research Objectives

The main objectives of this work are:

- To develop a mechanism for self-regenerating network software failure.
- To model the system using biological inspired mechanism which is cell internal operation and molecular production from DNA.
- To develop a technique to maintain the availability of a system over time.
- Generalize the attack detection to detect different kind of attacks.
- Develop the self-regenerative model based on multi-agent paradigm.
- Experiment the prototype model to ensure the interoperability of the agent.

1.5 Contribution

As contribution we are developing a system that is regenerative and self-managed, system that content efficient algorithm for dynamic regeneration in the presence of known and unknown anomalies. We can have the system manage itself without human intervention.

1.6 Thesis Structure

Throughout the thesis we have five chapters, the first chapter we explain certain key point of the research which is the problem statement and objective of this research as well as the research contribution and approaches. In the second chapter we have the literature review which includes bio-inspired current research activities and self-management trend. In chapter three we discuss our model that we have proposed and we did some theoretical formulation. In chapter four, we implement our model using JADE tool. JADE is java agent development framework used to model certain agent based system. In chapter five is the case study we took peer to peer as a first case study, the second is cluster network. We test our model in the two abovementioned case study and we present a result based on them. Finally, chapter six draws the conclusion of the research and recommendations for future work.

1.7 Research Approach

We used agent as a technical approach in the model, we implement four agents respectively as monitoring, replication and configuration, prevention, and run time management. These agents send messages accordingly in order to regenerate component.

1.8 Methodology

To ensure smooth progress of the research the following method and strategy will be applied:

- Explore the procedure of self regenerating mechanism and techniques.
- Study the attack detection and propagation.
- Model analysis and specifying, and the algorithm for the model using cell internal operation and molecular production from DNA, and model the algorithm using multi-agent paradigm.
- Compositional and simulations.

1.9 Scope

We address in our research certain characteristic of self-regenerative system, self-regenerative has the ability of learning environment and potential change or attack, and regenerate themselves, and automatically improve their ability to deliver critical service. The following in the scope of this research:

- Investigate and analyze a biologically system which has the ability of self-regenerative.
- To formulate a self-regenerative structural design by using biologically inspired architecture.
- Design survivable networked software using multi-agent paradigm.

1.10 Subject

The subject of this thesis is autonomic computing using biologically inspired self-regenerative software. Distributed system is the system that use distributed software which we consider in our research. We implement the cell regeneration into distributed software system to get self regenerative system in case of a failure of the system caused by anomalies.

An idea based on automatic computing concept has been presented in an attempt to maps the DNA self regeneration behavior to software system. Preliminary model for Network software self-regeneration is illustrated. We implement a mechanism to detect instruction that would cause the breakdown of software, this mechanism is based on multi-agent that work together in order to detect and to evaluate and to analyze potential harmful software execution. This outputs is a self-regenerative model using biologically inspired extracted from cell and DNA system structure and regeneration, of distributed network software and.