Survivable Networks

Sundeep Selvaraj Pundamale
Department of Computer Science
University of Helsinki

Abstract -The term survivability is defined as the capacity of a system or network in a working state to provide the essential services under the deterministic set of values. Most of the networks are unbounded, meaning that they do not have a central administrative control and a unified security policy. The discipline of survivability can help such unbounded systems to deliver essential services and maintain essential properties such as integrity, confidentiality and performance despite the presence of failures. Self-aware management allows the network to react and adapt to the changes inside the network system. This paper describes the survivability approach to a system that functions in a unbounded network and lays emphasis on how the self-aware architecture manages IP QoS guarantees. It also includes the challenges faced by a survivable wireless networks and the techniques used for self-healing in wireless network.

I. Introduction

During the last two decades network systems started gaining its significance drastically. Most of the educational institutes, financial services, health sectors, transportation, telecommunication companies etc now operate on a domestic, national and international level. They rely heavily upon these network systems to carry out their mission on a wide scale or a global level.

As the demand for network systems started to raise people realized the consequences of a failure in network system. Therefore some proactive measures are taken so as to increase the availability of these critical network systems. The availability of a system can be increased by acquiring the system services precisely and recover those services in a timely manner when there is a failure, attack or an accident.

Automating the supervision of these network systems become very crucial due to various factors..The demand for quality of service by the users increased and there is a cost involved to hire experts to maintain the network systems as per the users demands. Therefore it is important to reduce the human intervention in the network management and increase the automation of network process. This is often referred to as a control plan. And increasing the automation in Network Management is referred to as Management plan [2].While designing these plans it is very important to evaluate the operational objectives of the network system. It should also be enabled with respective monitoring and adaptation techniques.

As the global Internet started to evolve maintaining survivable networks efficiently proved to be more difficult. Because, there is a lack of central administration and the maintaining security is more complex in an unbounded network [1]. Though there is lack of central administration in these kind of networks, autonomous administration is effective when done carefully.

This paper describes the importance of boundaries in a survivable network. The key characteristics are described with appropriate examples. It is followed by self-aware management which helps to reduce the human intervention in handling a network . A policy based QoS management helps an operator to establish service objectives and policies in order to implement the network resources in future. An agent approach allows one to build a complex and sophisticated system using modular components. .A self-aware system has the ability to manage the processes itself. The architecture of self-aware management describes different levels which include the access mediator, service mediator, resource mediator and network elements.. A survivable wireless network has different set of challenges due to the fact that wireless communication travels through unpredictable medium unlike the error free transmission provided by cables. Security is an essential feature of survivable networks. Security has its own definition in survivable systems. It is further explained in this paper with an example how security and efficiency of a system is maintained.

II. The Domain of Survivability

While designing a survivable system it is important to understand the computing environment with in which the survivable system operates. The computing environment can be classified into two broad categories namely bounded and unbounded network infrastructures.

In a bounded system all the system parts are controlled by the a single administrative body and can be fully controlled. In an unbounded system there is no unified administrative control over the parts of the system. Here administrative control means having the authority to implement certain actions in the network rather than just being a member who recommends different solutions. In an unbounded system each participant has an incomplete view about the whole system so one has to depend and trust on its neighbors. Also a participant cannot have control outside its own local domain. A single unbounded

system can contain a collection of bounded and unbounded systems connected together in a network. Figure 1 shows the unbounded domain consisting of a collection of bounded systems which has its own administrative control. There are three boxes representing different unbounded networks having their own local policies. These policies are exchanged to the other trusted systems ans these unbounded systems are viewed as a single bounded network.

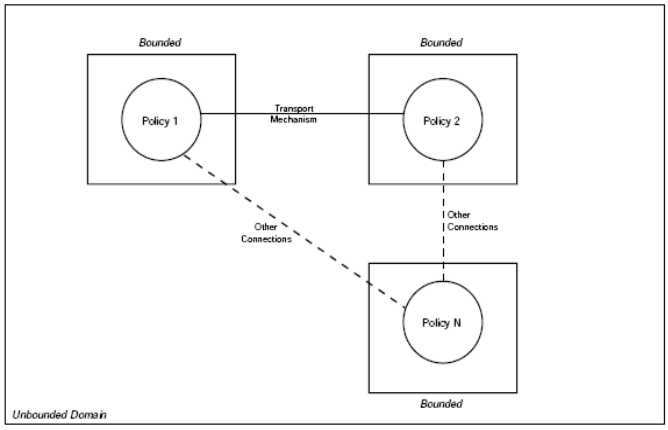

Figure 1 : An Unbounded Domain Viewed as a Collection of bounded systems

When an application is implemented in an environment which has multiple administrative domains the system is said to have an unbounded environment. For example the Internet can be viewed as an unbounded environment. The Internet is a collection of many client-server and network applications .In the case of a public web server its clients may lie within many different administrative domains on the Internet. There is no central authority that that configures all the clients in a similar fashion. Therefore a web server can never rely on the way a particular client is configured . In this example the web server and the its client form the system. The multiple administrative domains are the the variety of site domains on the Internet. Many of those domains have legitimate users. Other sites are used for intrusions in an anonymous setting. These latter sites cannot be distinguished by their administrative domain, but only client behavior. The interoperability between the server and its client is defined by a hyper text transport protocol which is a convention agreed upon between server and clients [2]. The system which composes of web servers and clients is geographically distributed widely through out the Internet. Both the legitimate users and attackers are part of the same environment and it is difficult to isolate these legitimate users from the the attackers. In other words it is quite difficult to bound a environment only for these legitimate users under a common administrative policy. Therefore security is considered to be a key factor in todays survivable network.

III. Characteristics of Survivable Network

One of the important characteristic feature of survivable network is their capability to survive and provide the most essential services even in case of a failure [2]. While delivering the services the system should also maintain some essential properties like specified levels of integrity, confidentiality, performance and other important quality attributes [1].For example a missile launcher is no more effective if the target is out of the range of the missile before it can be launched. These quality attributes play an important role.

The definition of survivability is often expressed in terms of maintaining a balance among multiple quality attributes such as performance, security, reliability, availability, fault-tolerance and modifiability. The ability of a system to deliver essential services, while maintaining its essential properties is to sustain even if a significant portion of the system is not functional. Also the capability of a system should not be dependent on the survival of a specific information resource, computation or communication link..The next important factor of survivability is to identify the essential services and the essential properties that support them within a particular operational system. *Essential service* can be defined as the functions of the system that can be maintained in case of a failure or hostile environment. For example in a military environment the *essential services* might be to maintain the technical superiority and *essential properties* might be to maintain integrity and confidentiality [1].

In a public sector a survivable financial sector is the one that maintains integrity, confidentiality and availability of essential information such as account information and loan data information and financial services like transaction validation and processing, even if a particular node or communication link fails due to some attack or an accident. It must have the ability to recover this compromised information and services in a timely manner. The important functionality of the system is to adapt itself to the environment and deliver the essential services. The ultimate idea is to fulfill the mission of the system just not making a portion of a system functional at all times. For example the essential services of a power delivery plant might be to distribute both electricity and natural gas. In this case the system is said to meet its mission if both the services are delivered in a timely manner. If either of the essential service is lost due to some reason it should be replaced by another service that supports the systems mission fulfillment in a different but equivalent way.

IV. Policy-based Qos Management

The Policy-Based Management (PBM) separates information

related to control of resources and information related to their states. It allows an operator to establish service objectives and policies that are implemented by the network resources in future. Thus the decision on resource allocation and configuration can be taken locally in an autonomous way.

The Policy-Based management defined by the Internet Engineering Task Force (IETF) proposes an infrastructure to manage IP networks offering service guarantees [2].The infrastructure proposed in the reference manage IP networks offering service guarantees. This infrastructure also allows a flexible behavior of the network. In other words it reacts to various events in the network based on the policy defined. These policies are nothing but a set of rules that are applied to the management and control of access to the network resources. They also allow the network administrators or the service providers to manage the networks behavior based on certain criteria like user identity or the type of application. Policies can also be defined at different levels. For example the highest level policy can be a business level policy that is translated further to a network level policy and then into a low level policy which is understandable by the network element.

The Internet Engineering Task Force (IETF) in collaboration with Distributed Management Task Force (DMTF) came up with a new model called as Policy Core Information Model (PCIM) [2].In this model the network is considered as a state machine where the policies are used to control the state transitions. It is capable of identifying the states and monitor their progress. This model also defines the role priorities and execution order.

V. Agent Approach

An agent approach is one of the promising feature in the survivable network. The agent approach allows one to build a complex or sophisticated system using modular components. The intelligent components are often referred as agents and the interaction among these agents is considered as the heart of the multi-agent system. An agent can be a simple software which is responsible for the execution of a process within the network. It might also have intelligence to automate some task.

In general intelligent agent is responsible to maintain a cooperation between the user interfaces and the intelligent processes to carry out some common task. Thus the agents are responsible to detect and solve the faults and maintain the infrastructure as they are expected to be. These properties are autonomous but also responsible for adaptation and distribution of the network. They allow automatic control and offers the services as per the users need. The presence of agents makes the network smart i.e it makes the network adaptable to some new situation and manage the services as per the conditions of the network system.

The agent based approach is mainly concerned with the introduction of mobile agents that are responsible to handle the dynamic nature of the network system. A mobile agent is generally an independent program which acts on behalf of the user and is capable of moving from one network node to the other. The important aspect of this approach is to negotiate with other processes and delegates work to other intelligent agents in order to reduce the load of communication in the network. The agent normally transports a business policy so that the negotiations and the decisions can can be carried out locally. The significant properties of the agent lies in its mobility and the capacity to negotiate [2].

VI. Architecture for Self-aware management

Self-aware management can be described as the ability of the management processes and the respective network infrastructure to maintain themselves with out the intervention of some external assistance. The role of the administration is just to layout the network operational structure. In order to offer this self aware management it is important to consider the dynamic nature of the underlying network infrastructure that should be managed [2]. The following four structures are the basic elements of a self-aware management system :

- self-configuration: The ability of the system to configure automatically with some high level policies.
- Self-optimization: The ability of a system to improve the performance and effectiveness of system and system components automatically.
- Self Healing: The ability of a system to detect, diagnose and repair the software and hardware components automatically.
- Self Protection: The ability of the system to protect itself from attacks and rollback from failures. The system failures are captured and alarms are generated.

An autonomic system known as a self managed system consists of autonomic elements known as self managed elements. These elements provide services to the end users and other autonomic elements. Also they are responsible to manage the state/behavior and controls the interaction of the elements with the environment. The self managed elements are referred to as *Agents* in this paper.

The architecture of self-aware management is built by using the concepts of policy based management and multi-agent systems [2]. This kind of architecture allows the dynamic Quality of service management within the framework. It is also in conformance with the architecture of the IST CADENUS (Creation And Deployment of End User services in premium network) project[2]. This standard came up with a Service Level Agreement (SLA) based on a frame work for

providing the appropriate services to the end users. The SLA defines the standards that a customer is expected to get when he subscribes with a service provider. This customer can be a user or another provider offering the same level o f service some times also called as a horizontal SLA. The customer might also be a service provider whose offer is at a different level which is referred to as a vertical SLA. The major part of the SLA specifies the services that must be delivered. The Service Level Specification is the technical part of SLA. It also contains the services description in technical terms.

The CADENUS project recommends the use of three levels for telecommunication services, the Access mediator, Service Mediator and Resource Mediator. The Architecture described in this paper includes the above mentioned three mediators. Also some new monitoring functions are introduced to allow each policy level to adapt its behavior with respect to the network that it is controlling. Each level is a self managed entity .Therefore it has the ability to provision services on its own with out much human intervention. The level of autonomy required is reached by introducing the operational objectives and the parameters to be followed in the infrastructure, as well as by providing respective monitoring and adaptation means. The necessity to use management system decreases and the operator does not need to apply corrections and adaptations so much any more. Thus the management system is simplified and is more oriented towards the definition of policies and operational parameters. Each level implements their own method of monitoring and have a meta-control level which allows to adapt its behavior to the dynamic nature of environment. The meta-control level contains two categories of agents :

- The Monitoring Agent: It controls the adherence of networks or the network elements behavior with the policies that were applied earlier.
- Adaptation Agent: It modifies the mediator/network. Element behavior in order to improve its operation performance and to optimize the service configuration.

Each level is explained in detail in the following sub-sections:

A . The Access Mediator:

The Access Mediator is mainly responsible for the cooperation between the end-user and several service providers. It has knowledge about the end-users,access link,terminal type and gives them access to particular service provider. The Access Mediator provides a user with a wider selection of services at the lowest cost. It also simplifies the process of service selection. It can also immediately notify the user when a new service becomes available. A mobile agent is used for dynamic negotiation of SLA between customer and several other Access Mediators.

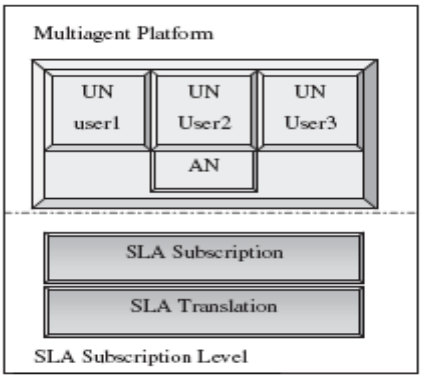

Figure 3. Access Mediator [2]

An agent called User Overseer (UO) is located on the users terminal. It sends the mobile agent called User Negotiator (UN) to the Access Mediators in order to negotiate the services according to the users needs. They now send the User Overseer about the results of their negotiation as well as the new offers that may interest the user. The User Overseer now selects the best offer among the services it received. An agent called as an Access Negotiator (AN) negotiates services and provides the classification based on on behalf of the Access Mediators.
The Access Mediator contains a multi agent platform and two access modules namely :

- SLA Subscription: The SLA subscription is an agreement between the customer and the service provider upon certain QOS parameters. It also helps the service provider to precisely identify the needs ot the customer from this document.
- SLA Translation: It translates the new service request into an XML format and sends it to the Service Mediator Concerned.

B. The Service Mediator

The Service Mediator is responsible for informing the acces-mediators of all the new service offers. It is also responsible for the management of the physical access to the services through the appropriate underlying network using the resource mediators concerned. The Service Mediators do not have a direct contact with the end users for SLA. It deals with other service providers to compose its services and with network providers to support its services.

C. The Resource Mediator

The resource mediator manages the underlying network. It is responsible to maintain the network performance as per the demand of the the service providers. In a policy based management environment it plays the role of a Policy

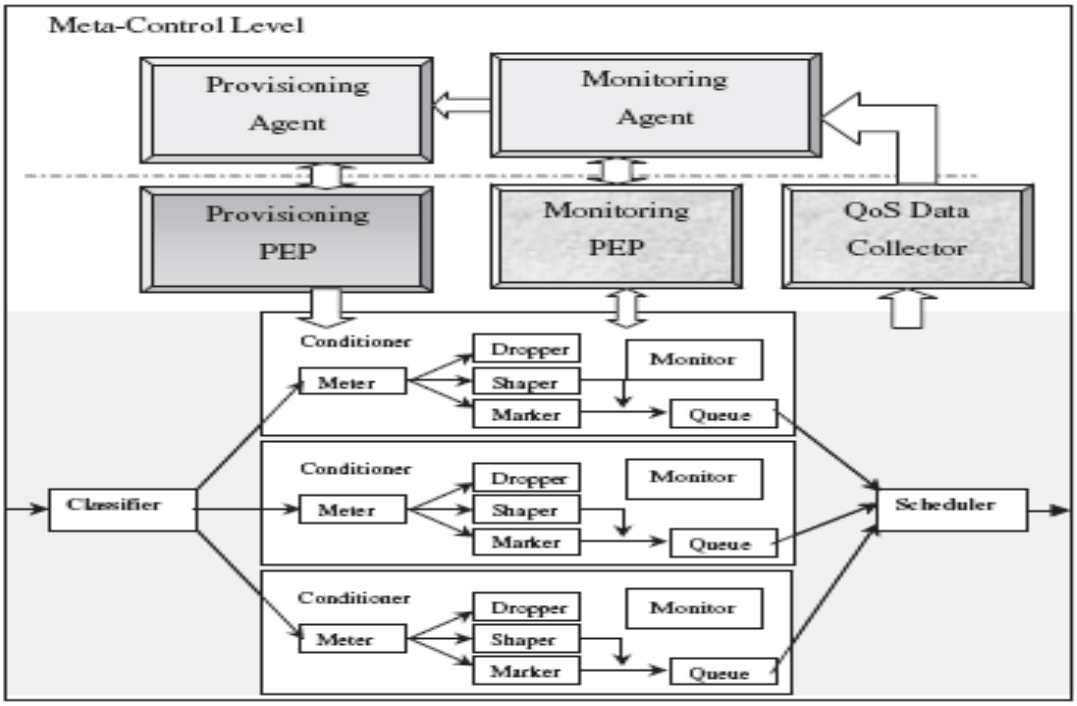

Figure 4 Network Element

decision Point (PDP). It now has the responsibility to identify which policy rules are applicable to the network elements that satisfy the service mediators. The main role of PDP in this architecture is to send the network level policies that cannot be directly executed by the network elements. Policy rules are generally of the following type :

Policy : Service Configuration
For: Edge Router 1
On : Source IP Address
Do : PHB type

D. The Network Elements :

Each network element has a local Policy Decision point (PDP) and Policy Enforcement point (PEP). The PEP has the application point of policies. It is also responsible for packet filtering,bandwidth reservation,traffic priority etc. The local PDP receives the decisions and the policy rules from the Resource Mediators (RM) and translates these policy rules into policy rules or commands which is understandable by the PEP. To do that it has an information database that contains the different policy rules to be executed according to the decisions received from the RM and its perception about its environment. Figure 4 mentioned represents the network element. A network element consists of 2 modules to implement the policy rules :

- Provisioning PEP : It is used for enforcement of provisioning for policy rules.
- Monitoring PEP : It is used for configuration of monitoring tools.

Also each network element includes a Meta-Control level consisting of two agents, the Provisioning agent and the monitoring agent. The major role of the provisioning agent is to push the new configuration rules to PEP depending on the network state and the policy rules sent by the RM.

VII. Survivable Wireless Networks

Unlike the error free transmission provided by cables the environment the that wireless communication travels through is unpredictable. To name a few environmental radio-frequency (RF), noise produced by powerful motors, other wireless devices, micro waves and moisture content in the air can make the wireless communication unreliable.

Generally the wireless networks follow the traditional wired models and are manually configurable. This means that to join a particular node or a transceiver enabled device it must be programmed to direct its communication to another particular node which is generally a central base station [5]. The biggest challenge here is that if the node looses contact with its designated peer the communication ends. In order to compensate this drawback these nodes where placed in the optimal space. However even this decision also could not guarantee reliability as the environment can change from day to day.

The most promising developments in the area of self-healing wireless networks is Ad hoc network. They are decentralized, self-organizing and automatically reconfigure without with out human intervention when there is some degradation in communication or broken communication links between the transceiver. These networks may have bridges or gateways to other networks such as wired Ethernet or 802.11.The major strength of this kind of architecture is that they do not require a base station or central point of control [5].

In the decentralized network each node acts as both a end point and router for other nodes. This naturally increases the redundancy of the network and increases the scalability of the network. Automated network analysis through link and route discovery and evaluation are the most prominent features of the self healing network algorithms. Through discovery netw-orks establish one or more routes between the originator and recipient of a message. Through evaluation networks detect route failures,triggers renewed discovery and select the best route available for the message.

Generally wireless self-healing network have pro-active or on demand discovery and single path and dynamic routing. These characteristics affects the network latency, throughput, reso-urce needs and power consumption in varying amounts. The pro-active discovery networks configure and reconfigure constantly. They assume that link breakages and performance changes are always happening and they are structured to continuously discover and reinforce optimal linkages. Proacti-ve discovery occurs when nodes assume that all routes are possible and attempt to discover every one of them. The on demand discovery in contrast establish only the routes that are requested by higher layer software. This allows the nodes to save power and bandwidth and keeps the network free from traffic. In case of a single path routing as the name suggests there exists a single route for a given source and destination. Some times even the end - to -end route is also predetermined. With the case of a Dynamic routing messages are broad casted to all the neighbors and forwarded according to a cost-to-destination scheme. Although this type of routing has the advantage of of multiple redundant routes from originator to the destination it generates lot of traffic on the network.

A. Self-healing techniques in wireless networks

The Gradient routing in ad hoc networks is an example of total dynamic routing. It is illustrated in figure 5 .GRAd's routing emphasizes on potential availability of redundant routes from originator to destination nodes to optimize for lowest latencies. To reduce the network traffic once the message has made it to the destination, GRAd suppresses the message loops by returning an acknowledgment The maintenance of multiple sets of routes adds memory cost and network traffic but the return is an increase in both reliability and speed of message delivery [5].

VIII. Survivability and Security

Computer security is often treated as binary. Which means at any given time a system is either safe or compromised. But this definition of security does not hold good in survivable networks. As per the definition of a survivable system the systems component must collectively accomplish their

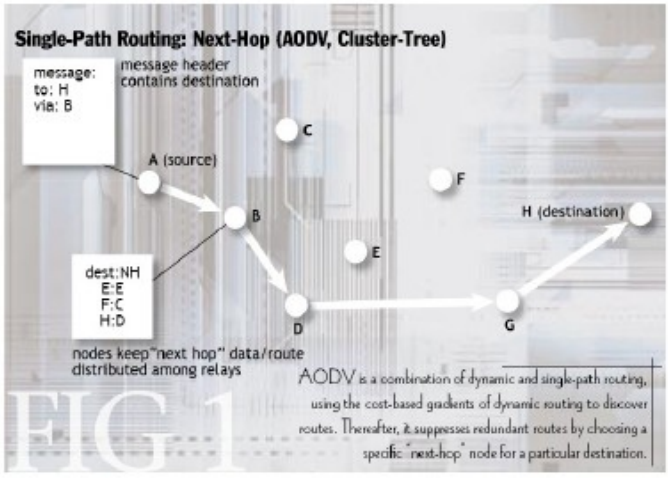

Figure 5 Gradient Routing in ad hoc network

mission even under attack and intrusions that can damage the significant portion of the system. Here is an example that assumes the survivability of a network to be yes or no under a given scenario. Figure 2 shows a representation of N/Node unidirectional path switched ring. The availability, A of the existing system/network can be calculated based on the past performance data. However to predict the availability of a new system probabilistic approach can be used. Unavailability is the complement of availability i.e (Unavailability=1-Availability).A system network Unavailability is expressed in minutes per year or U=MTTR/MTBF where MTTR is the mean time to repair from a failure and MTBF is the mean time between those failures. [3]

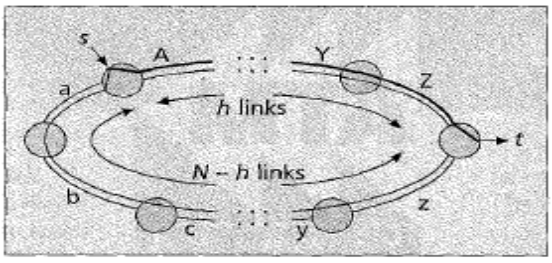

Figure 6. N-node unidirectional path switched ring

It would make sense to restrict the discussion of this example to Unidirectional communication instead of bi-directional circuits because the discussion for the reverse direction from T to S (two nodes communicating with each other as represented in figure 2) is practically same as S to T . Also both directions of a given transport signal generally traverse through the same set of links and nodes between S and T. Hence the service availabilities of both the directions can be assumed to be mathematically identical and the bidirectional service availability can be assumed to be mathematical intersection of these two directions. In the Unidirectional path switched ring the transport signal is duplicated at the originator node S and transmitted onto both the directions of the unidirectional path switched ring such that two copies of the transport signal are presented to the patch selector at the destination node T. In this model we assume the upper path as service path which traverse through h links of the N nodes in the unidirectional patch switched ring. If a link or node along this h link path between S and T fail the path selector at the destination node T would perform a path protection switch to receive the copy of the transport signal arriving via the N-h link lower path and thus restore from failure. Once the failure is repaired the path selector can be reversed such that it is switched back to the upper path or if the failure continues, the path selector selects the lower path connection which then becomes the new service path. Thus the service bearing transport signal survives even if one or more intermediate links or nodes along the path 'h' fails.

The above example captures all the failure scenarios and makes the model mathematically complete. Robustness under a attack plays a vital role here. Robustness in particular can be compared to recoverability which is also an essential characteristic of survivable systems. In the policy based management intelligent agents are also used to implement security policies. The security management in a system is divided in to three plans :

- User plan
- Intelligent plan
- Network plan

In the user plan the administrator defines the security policies to be applied in the network. The security policy is built in such a way so that when there is an attack , the system has to detect and also guide the agents behavior. The intelligent plan is the intelligent part of the system. It is formed by one or more multi agents. The network plan represents a network. It is responsible to collect various events related to security with in the network, analyze it and based on it future attacks are prevented.

IX . Conclusion

In this article results were selected from the recent research including the modeling of various self-healing architectures in order to compute the service ability, QoS guarantees which allow self configuration,self provisioning and self monitoring services. The agent concept described in this paper enables automation which is a key functionality of survivable networks. Despite of the best efforts in maintaining security in unbounded networks. The discipline of survivability help to tighten security in unbounded networks. There are further promising research areas in Survivable Network.

XII . References

[1] R.J Ellison, D.A Fisher, R.C Linger, H.F Lipson, T Longstaff, N.R Mead,Survivable Network systems,November 1997.

[2] Francine Krief, Self-aware management of IP networks with QoS guarantees,pg 351-364,2004

[3]Mark R Wilson,“The Quantitative impact of survivable Network Architectures on Service Availability”, IEEE communication magazine may 1998.

[4] R.C.Linger, N.R.Mead and H.F.Lipson “Requirements Definition for Survivable Network Systems”, Carnegie Mellon University.

[5] Robert Poor,Cliff Bowman, Charlotte Burgess Auburn, Ember Corporation, ACM queue vol 1,may 2003.