Position papers of the 2014 Federated Conference on Computer Science and Information Systems pp. 165–170
DOI: 10.15439/2014F459
ACSIS, Vol. 3

Dynamic Autonomic Network Management: Evaluating the Architectural Challenges of Autonomic Management for Mobile Ubiquitous Access

[1]Clifford C.L Sibanda, Olabisi E. Falowo

Department of Electrical Engineering,
University of Cape Town,
Private Bag X3, Rondebosch 7701 :
[1]clifford@crg.ee.uct.ac.za

***Abstract*—As technology rapidly improves there is more mobile and portable devices available on the market, making the prospects of ubiquitous access to Information Communications Technology (ICT) services a bigger better reality every day. The major hurdle which is the ICT skills shortage can be solved by using autonomic management of the devices on the network and end user equipment. Network and application service providers competing to retain the customer base in order to maintain a guaranteed and healthy income, need to improve network management and stick to service level agreements. This can easily be achieved through enabling network components to automatically configure and optimize their settings, operations and performance. Autonomic network and device management has great advantages including, reduction of human error, reduction on the dependency of the scarce and expensive human skill and much faster introduction of applications, new services and technology, saving the critical and scarce time. However, due to architectural differences major problems arise when a mobile node traverses heterogeneous networks and systems that employ different management paradigms different aspects for similar processes such as Call Admission Control (CAC) mechanisms, Quality of Service (QoS) issues and Security.**

***Index Terms*—Self-configuration, Self-optimization, Ubiquitous access, Mobility, Heterogeneous Networks**

I. Introduction

THE LAST few years have seen rapid developments in technology on both the network side and the devices side. However the speed of the proliferation of high-tech devices to the ordinary user has not and could not be matched by the human Information and Communications Technology (ICT) skills available in the world [1]. Thus configuration management is often left to the poor user who parts with hard earned cash only to enjoy the access to service, data, information, entertainment and the entire digital tech world can offer. The level of skills possessed by the average ordinary user is far less than enough to adequately and optimally use the ICT resources available

The proliferation of the complex, altogether different yet complimentary heterogeneous networks introduces yet another angle that leads to user confusion and inefficient use of resources available. Ubiquitous service access by mobile users across heterogeneous systems, without the bother of changing settings or devices is desirable.

Human interface in network management is hampered by several aspects including but not limited to the already mentioned worldwide shortage of the trained ICT personnel. Human operations are prone to errors and sometimes poor judgment leading to unavailability of ICT resources to impatient end users.

Also, as service providers compete to retain the customer base in order to maintain a healthy income, the need to increase the up time of the network for users to easily access ICT resources is high. On the user equipment side the need to lessen the burden on the user is also desirable, through some means of automation that would make access to service easy and fast.

The need to avail all the new services as soon as possible is extremely unavoidable. One such route to be used to achieve this end is to allow the network and devices to automatically configure, heal, protect and optimize their performance. Thus the introduction of intelligence in the end systems as has been done ` to the core network systems is very vital to ensure the take of autonomic management of the systems.

Some problems arise when a mobile node traverses heterogeneous networks and systems that employ different management paradigms as shown in Figure 1, with different aspects for similar processes such as Call Admission Control (CAC) mechanisms, Quality of Service (QoS) issues and Security [7] [9].

The remainder of this paper is organized as follows: In Section II, we discuss the concepts of Autonomic Computing/Management, in Section III, we discuss the challenges that we identify as related to the Architecture of networks that need addressing if autonomic management is to take off. Section IV contains our suggested research areas for solutions to the challenges and Section V discusses related work.

II. Human administered Network management & Autonomic Computing

Network Management administered by human beings can be viewed as a full time occupation that involves the deployment, maintenance, optimization and upgrade of network components. Deployment would normally involve installa-

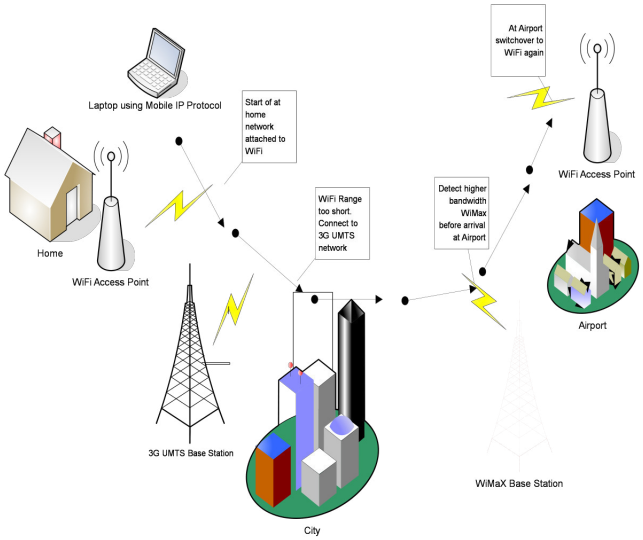

Fig 1. Mobile Heterogeneous Network Access

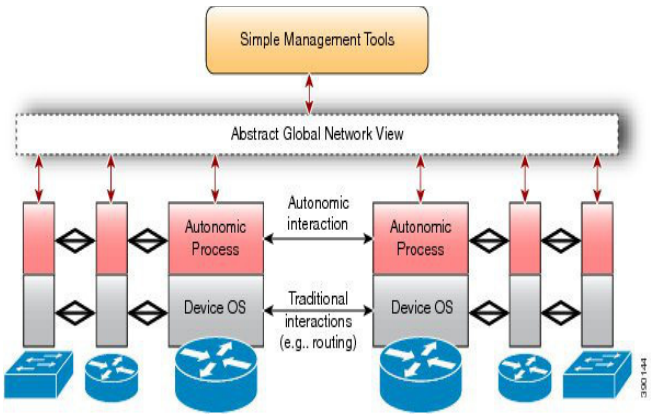

Fig 2. Use of Simple Network Tools with Autonomic [19]

tion, loading of software to interface between the machine and the human, configuration and commissioning the network. Hundred percent uptime of the network is impossible especially if it is in use, hence maintenance is needed. Maintenance could be carried out pro-actively, i.e. to prevent faults from occurring or reactively, i.e. resolving faults that have occurred.

Optimization is generally the changes effected to maximize the gain from the use of the network, as network variables, environment and performance changes on the fly, the need to optimize the network usage is best dealt with using autonomic means. Whereas upgrades effect changes to improve aspects of the network e.g. introducing new drivers or system software that allows for increasing the link speed from 384kb/s to 1Mb/s, these upgrades when automated and occurring in the background allow users to carry on using the network with the prospect of better network experience once the upgrade is complete.

The human dependant network management requires highly skilled personnel to carry out the deployment, maintenance, optimization and upgrades of the network. Accepted, there is a shortage of these skilled ICT personnel to carry out these tasks, hence the need to automate most of the work. Moreover due to the shortage, the highly skilled ICT personnel are in great demand; hence the market offers good remuneration, making them highly mobile. The mobility of the highly skilled ICT personnel at time causes problems as they move with critical network information that they would have gained over the time of their administration.

Also because human beings cannot be at work 24 hours a day, some faults have to wait for a specific person to be on duty for it to be resolved. Human Intervention network management is dependent on the use of tools (shown in Figure 2) that an engineer/network administrator or technician will occasionally consult to make decisions on the status of the network. The frequency of the consultation may also be factor in the status of the system at any given time.

Common tools used by network administration personnel range from protocols such as the Simple Network Management Protocol (SNMP) to Application software on open resources hardware or firmware to those on proprietary hardware and firmware such Cisco equipment using Cisco proprietary hardware, firmware and operating systems. The tools can also include the methodology of network administration, for which several academia papers are available [15], [16], [17] [19].

Network administration management can be classified in different ways such as: the passive versus active network management as well as distributed versus centralized network management.

Passive network administration refers to network administration in which network logging and network configurations are carried out such that they do not affect network operations. This could mean the logs analysis is not real time or online. On the other hand, active network administration refers to real time network logging, configurations and adjustments.

Centralized network administration refers to network management that is guided by one entity or same policies sometimes from a single point. On the other hand, distributed network administration refers to several points/centers of network management and policies creation and implementation.

Autonomic network management refers to the ability of the network to manage itself with minimal human intervention. It is a branch of the Autonomic computing paradigm, and it owes its existence to the Integrated Business Machines (IBM), efforts in the 1990s known as Autonomic management [4]. The efforts of the research in this area have not to date yielded much industry usable solutions.

While the computing and network management area has made great strides from the era of extensive and difficult command line interfaces to Graphic user interface and Web based interfaces, it was not until the introduction of policy based network management ideas that the realization of autonomic network management was any closer to reality.

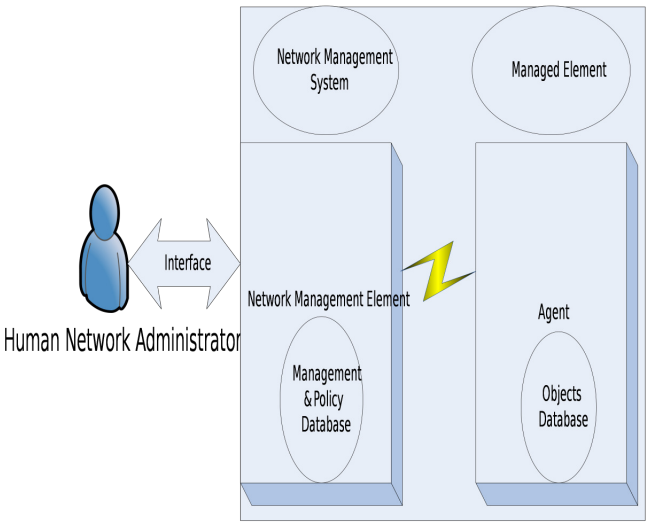

Fig 3. Human Interface Network Management

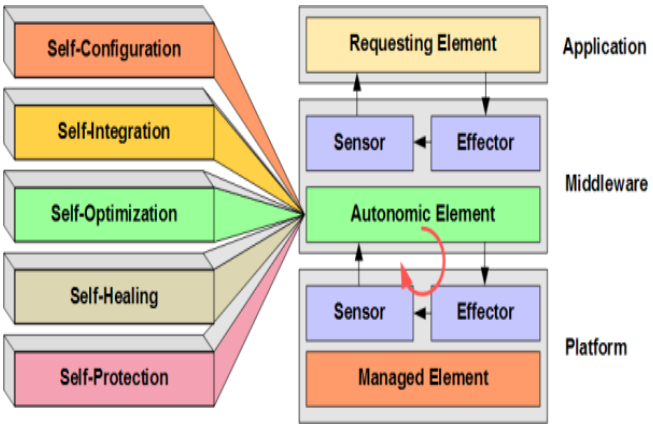

Fig 4. Main Self-Areas of Autonomic Management

Autonomic network and device management has several advantages to both the user and the service provider including saving the critical and scarce time, reduction of human error, reduction on the dependency of the scarce and expensive human skill and much faster introduction of applications, new services and technology.

The general principles of autonomic management as envisaged by pioneers of this research paradigm, who included IBM, identified 4 main areas namely self-configuring, self-healing, self-optimizing and self-protecting aspects of automatic management by devices. Several other areas have emerged as research in this arena continues with aspects such as self-aware, self-organization, self-preservation and self-locating, Self-Integration[5].

The four major aspect of Autonomic Network Management Self-CHOP can be as indicated below.

Self-configuration is meant to allow devices to change their configuration as is dictated by the situation and environment.

Self-healing is meant to allow devices to take corrective measures for any systems states that could cause malfunction and disruptions.

Self-optimization is meant to allow devices to take advantage of resources available to the maximum ability

Self-protection is meant to allow devices to enforce appropriate security policies in the event of attacks or perceived intrusions that can cause denial of service or destructive action that can cause loss of service [4].

III. Related Work

Autonomic Network Architecture (ANA) project seeks to develop a network architecture that can self-organize [8]. The research explores ways of organizing and using networks beyond the current Internet technology. The goal is to design and develop a network architecture that is flexible, dynamic, and fully autonomic as a whole. The developed product should be dynamically adaptable according to the working, economical and social needs of the users. One key attribute is that the developed network scales, in a functional, easily extending both horizontally (across systems) as well as vertically (as a solution) [2].

Mobility First Future Internet Architecture is part of a bigger project being undertaken in America that seeks to redesign the Internet based on the mobile nodes as opposed to the legacy Internet architecture based on in-situ servers [3]. The projection of this study is that mobile application platforms will replace the fixed application platforms by 2015. With a vision of a future internet that supports mobile devices as ‘first class’ objects, the need to have the mobile nodes operate efficiently, accurately and autonomic is very high.

FOCALE (Foundation Observe Compare Act Learn rEason): This is a distributed architecture that mainly depends on Autonomic Components (AC), where each AC can incorporate the autonomic management functionalities. The main challenge for FOCALE is to accommodate legacy components i.e. already existing network components, and ensure that new Autonomically Enabled Managed Components can also be efficiently integrated and managed. The research also seeks to utilize policy based management of ACs. FOCALE provides a means to reason about the environment and recommend or take appropriate actions, so that the underlying business goals are not violated and, hopefully, optimized [12]. Using sensors to gather information on the environment, FOCALE seeks to implement context-aware policies to change behaviour of Autonomic Components [13] [14]. The context aware policies in our view are relatively closer to achieving SLA honoring. There is need to extend the work in [12] and [13] to ensure enforcement of the SLA within the context of user’s immediate environment. In cases of nonexistent SLA’s or lack of QoS mappings to take care of SLA’s on demand autonomic SLA configurations should be possible.

BIONETS are biologically inspired networks. The human biological system has a stable autonomic system that carries out self-management tasks that ensure balance in the body

and thus preserving life [1]. Biological ecosystems also have ways of balancing very complex natural environments. Natural ecosystems tend to balance large populations of diverse organism while efficiently achieving equilibrium through collaboration and competition, yet there is no central controlling entity to organise or manage the equilibrium. The BIONETs project seeks to use the natural systems characteristics to create autonomic networks capable of also managing themselves similarly [6].

IV. Challenges for Autonomic Network Architectures

f devices are enabled to autonomically manage their configuration, state and operations, changes could be effected because of changes in the environment or changes in technology e.g. software updates or version changes. The ultimate goal of the changes is enhanced user experience or more efficient usage of resources or even accommodation of more users for the same service. Changes may include bug fixes or enhanced versions or changes in spectrum used or bandwidth used by devices.

The possibilities of a non recoverable error should total control be left to the devices to change their properties, is also a real danger and thus implementable solutions should allow for recovery and rollbacks. Recovery and roll backs would efficiently be implemented if the devices had enough memory to keep current state before accepting the new state, but the majority of the small devices accessible to users such as cellphones and body area sensors have no memory to hold two different images of software.

In the past few years the speedy convergence of Telecommunications networks and data networks saw an unprecedented upsurge of new applications that readily utilize the advantages offered by the convergence. The major success and effective key driver of convergence, being the phenomenal Internet. Spurred by the all IP networks capable of carrying all kinds of traffic ranging from voice, data to video, the converged network has brought further difficulties in network management.

As such the Internet Engineering task Force (IETF) has been kept busy with modifications of standards, proposals and drafts that help in the management of the Internet. The constant modifications clearly indicate the difficulty in which the current and future applications fit into the originally envisaged architecture of the Internet. There has been a massive increase of the Internet Servers putting the ever questioned lack of central control of the Internet out of the question as it were.

In general the rigid nature of architectural layers of the Internet such as the TCP/IP suite protocols, have literally meant modifications of as many protocols at each small change on the way nodes access the Internet. Several cross layer optimization and workaround solutions have been suggested [11]. However the cross layer solutions have no guarantee of ability to function for the future Internet.

Ad-hoc, mesh and distributed architectures have proved even more popular as the Internet continues to grow, thus the centralized and hierarchical architecture are not the core of the Internet anymore and the future architecture is strongly distributed with high possibilities of the so called core being composed of mobile and ever changing nodes. This idea literally breaks the Internet as we know it and how it is was founded.

The concept of mobile nodes accessing the Internet encouraged a lot of research as the Internet success had for a long time been based on the ability for nodes to route packets via open routes using addressing which had to be static during the initiated connections [10]. The tunneling solutions that emerged attempted to maintain this state for the birth of mobile Internet. To help matters was that the mobile node was always assumed to be communicating with a static server. The future Internet presents even more uncertainty in that the server might be distributed amongst several autonomic nodes which might all be mobile, moreover with no co-ordination whatsoever of the group mobility of the server.

In general the rigid nature of architectural layers of the Internet such as the TCP/IP suite protocols, have literally meant modifications of as many protocols at each small change on the way nodes access the Internet. Several cross layer optimization and workaround solutions have been suggested [11]. However the cross layer solutions have no guarantee of ability to function for the future Internet.

Mobility across heterogeneous networks and systems with different architectures and design also makes autonomic management complex with very little hope of standardization across different proprietary vendor equipment. Call admission control poses a serious problem when it comes to heterogeneous access for mobile nodes.

V. Component Based Solution

This paper envisages the major solutions for the future Internet management will rely on the use of Components and objects as opposed to the hierarchical structures currently used. As such the distributed and flat structure of the network will eventually be realized through non homogeneous mobile nodes serving as both consumers and producers of the content.

Component and object based approaches in the ICT field have shown the advantages of the removal of the single point of failure, component re-use and distributed function value as opposed to centralized and heavily coupled functions. Distributed Components can be combined or re-matched as required. Component and objects upgrades, changes or upgrades can be done without affecting the on-going network operations. [18]

Components are elements that represent independent, interchangeable parts of a system. Components and objects in a system conform to or model one or more interfaces, which allow for the interaction and determine the general behaviour of components.

In general, using components makes a system more flexible, scalable, and reusable. Another advantage of components and objects is that they are replaceable without disrupting the entire systems

For a component to be replaceable, it must meet the following criteria:

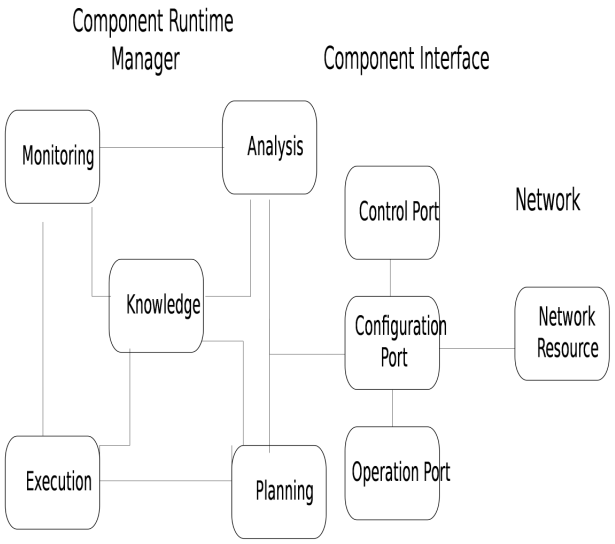

Fig 5. Autonomic Network Management Component visualisation [18]

- The internal structure of the component must be hidden. No dependencies can exist between the contents of the component and other objects.
- Components must provide interfaces so that external objects can interact with them.
- The internal structure of the component must be independent. The internal objects must have no knowledge of the external objects.
- Components must specify their required interfaces so that they have access to external objects.

In models that depict executable systems, components represent the components that are used during the execution of the system. Examples include COM+ objects, JavaBeans™, and Web services.

A component usually is named after the part of the system that it represents.

The boom of small distributed servers with content in the form smartphones, tablets, laptops and personal computers operating as the producer consumer internet client-servers and the current day distributed cloud technology renders little operations for the centralized management and human based management but rather favours the distributed automated policy based management. Business policy is translated into network, applications, storage policies that ensure smooth business operations.

This structure will inform the network management paradigms of the future. The distributed, non homogeneous, non enterprise structure of the network will effectively render the human interface of the network management invalid, but rather a set of policies working on open platforms that regulate access to specific services and groups, however possible resulting in frequent re-configurations by both the network and end user equipment to fit the circumstances.

Hybrid Hierarchal/flat IP Architecture and component based solutions could be the bridge between the current architectures and structures. The hybrid structures will allow for existing systems and structures to co-exist. The emerging systems which will through component based autonomic network management interact with the legacy systems using the hierarchical network management systems.

VI. Future Work

The open research areas that will see the ease of Autonomic Network Architecture design and development easier are not easily quantifiable now. Thus our discussion is not exhaustive but seeks to address the identified problems in this paper.

Desired solutions for Autonomic Network Management should answer the question of assurance of maintained original objective of the network node or the network as a whole as less and less human intervention is effected. This challenge coupled with the security concerns of a network and authentic changes being effected on the network could see the reluctance of industry opting for fully autonomic networks. Version control and verification models for fully autonomic systems are essential.

Control and security in peer environments are as crucial, as the need to fully co-operate in ensuring the flow of information. A balance model of co-operation and trust guidance is important as learning from the environment should not lead to poisoning.

The major solutions lie in the redesign and redefinition of network architecture. As opposed to the layering architecture was pushed by the TCP/IP model, a new component based model will greatly serve the future Internet. Cross layer solutions have attempted to give relief but will not hold up as services and applications continue to evolve in the Future Internet. Components are fully functional units that can interface with any other with a lot of ease. Object oriented components also allow easy re-use and plug-in adaptations.

Mobility as basic feature of the architecture for both the client and server is non-negotiable. Trends have shown a fade in the distinction of client and server, with the emergence of Producer-Consumer models also known as Prosumers. The idea stretches into the paradigm of client nodes being part of the management nodes of the network.

Resource Management and Allocation will take a different approach to please the ever versatile Prosumers market of the future Internet. Dynamic network changes will be the order of the day, but with the question of perceived user satisfaction prioritised. This calls for new call admission and QoS models that follow the changes in the environment

User preferences, profiles and contracts, are now more in the hands of the user than the network administrator and the unpredictable nature of the changes has an impact on the network configurations and operations. As more and more services and applications become available to the digital native users, dynamic autonomic management for the highly mobile, distributed and pervasive nodes, is the only solution.

References

[1] S. Hariri et al, "The autonomic computing paradigm", *Springer Science 2006.*
[2] H. A. Muller, "Autonomic Computing", *Technical Note - SEI-2006-TN-006, April 2006, Carnegie Mellon University*
[3] Online - http://mobilityfirst.winlab.rutgers.edu/Vision.html

[4] “An architectural blueprint for Autonomic Computing” , White Paper, IBM, June 2005. *Online http://www.research.ibm.com/autonomic/*
[5] Agoulmine et al, “Challenges of Autonomic Network Management”, *Proceedings of IEEE Workshop on Modelling Autonomic Communications Environments 2006*
[6] V. Simon, et al, “Bionets: A new vision of Opportunistic Networks”, *Proceedings of WRECOM 2007*
[7] L. Mokhesi, et al, “Context Aware Handoff Decision for Wireless Access Networks using Bayesian Networks”, *Proceedings of SAICSIT 2009*.
[8] C. Jelger, et al, “Basic abstractions for an autonomic network architecture”, *Proceedings of WoWMoM 2007.*
[9] G. Pujolle, “An autonomic architecture for Network Management and Control” , *New Network Management Trends, UPGRADE Vol. IX, No 6, December 2008*
[10] J. Redi et al, "Mobile IP: A Solution for Transparent, Seamless Mobile Computer Communications", *Upcoming Trends in Mobile Computing and Communications, 1998*
[11] X. Lin, “A Tutorial on Cross-Layer Optimization in Wireless Networks”, I*EEE Journal On Selected Areas In Communications, VOL. 24, NO. 8, AUGUST 2006*
[12] J Strassner et al, “FOCALE: A Novel Autonomic Networking Architecture*”. Proceedings of Latin-American Autonomic Computing Symposium (LAACS), 2006*
[13] J Strassner et al, “An Autonomic Architecture to Manage Ubiquitous Computing Networks and Applications*”. Proceedings IEEE Workshop ICUFN, 2009.*
[14] J. Strassner et al, “A Context-Aware Policy Model to Support Autonomic Networking”*, IEEE International Computer Software and Applications Conference 2008.*
[15] Dae-Young Kim, et al, “Ontology-Based Methodology for Managing Heterogeneous Wireless Sensor Networks,” *International Journal of Distributed Sensor Networks, vol. 2013.*
[16] Rupali Chopade, et al, Local Area Network Administration Using Mobile, *International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 3, March 2012*.
[17] Thomas A. Limoncelli, et al, The Practice of System and Network Administration, *2nd ed, Person Education, 2007*.
[18] http://acl.ece.arizona.edu/projects/old/Autonomia_ Programmable/index.html
[19] http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/auto_net/configuration/xe-3s/asr903/an-auto-net-xe-3s-asr903-book.html, *March 2014*.