International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Self-Healing and Resilience of Complex Network

Navin Dhinnesh ADC, Sabapathi T

Abstract*: Currently mobile operators spend more money towards maintaining the mobile network in fsinding faults, which will degrade the cellular services. If any fault occurs in the network it must be healed automatically and made to work. This self-healing network gives solutions for fixing or helps in deciding the problems to be carried out autonomously with no human interference. Also the networks ability to recover after any failure is said to be resilience. This paper discusses the strategy of resilience of complex network, its principles and metrics of resilience. The main aim of self-healing and resilience is to heal the network automatically and the network must recover after any fault.

***Index Terms*: Long Term Evolution, resilience, ResiliNets, self-healing**

I. INTRODUCTION

At present customers are expecting and demanding high data rates at low cost. The network operators are experiencing more stress in meeting the rise in expenses for the operation of cellular service [1]. The expenses met out by the cellular network operators are categorized as: i) Capital, and ii) Operational expenses. The former is spent for obtaining and updating network units. The latter is spent on the existing network reserves for running and maintaining them. The introduction of next generation of 5G technology has further augmented the data load on the network. To overcome this, 3rd Generation Partnership Project (**3GPP),** an organization developing protocols for mobile networks, deployed an automated process called as Self-Organizing Network (SON). This SON is further split into three: i) Self-optimization [2], Self-configuration and Self-Healing [3]. Self-optimization is mainly associated with mobile network performance, depending on the specification provided by the operator. Self-configuration refers to plug and play concept, which automatically organizes the mobile network. The main work of self-healing is to detect the cells which are not working, spot out the fault and their cause, and fix those problems for proper working [4].

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Navin Dhinnesh ADC*, Department of Computer Applications, Mepco Schlenk Engineering College, Sivakasi, India.
Sabapathi T, Department of Electronics and Communication Engineering, Mepco Schlenk Engineering College, Sivakasi, India.

When a new technology like Long Term Evolution (LTE) is deployed over the existing system, it should have the capacity to handle any complex situation of heterogeneous networks. Seeing the growth of mobile network, the network operators find it more difficult to maintain and operate the network without any fault. But they have to give good quality service and at the same time they see that operation expenditures are not increased. Self-healing comprises of three different phases for troubleshooting. First, the cells which are having faults or problems are detected. Second, for the faulty cells, revival measures must be identified. The root cause of the problem must be find out and analyzed. The root cause analysis takes two forms: i) fault identification – this will find the fault that is caused by key performance indicators (KPIs), and ii) action identification – this will give solutions to the problem. Third, the actions are executed by the re-energized cells. There is another measure called as fault compensation. The function of this is to minimize the fault and to reconfigure the neighboring cells. Compared to self-configuration and self-optimization, it is by self-healing the operation expenditures (OPEX) are marginally decreased by reducing the influence of mobile network outages [5].

II. HISTORY OF SELF-HEALING

Once the 4th generation (4G) cellular network was introduced, Self Organizing Network (SON) functions started to have gained popularity, since the 4G network was complex. A SON function is said to be effective with the following four key components [6]: i) Autonomy, ii) Scalability, iii) Adaptability, and iv) Intelligent [7]. The following table 1 shows the key components and its corresponding SON functions.

Table - I Key Components and its SON Functions

S No	Key Components	SON Functions
1	Autonomy	self-sufficient of human contribution
2	Scalability	able to change size (time and space)
3	Adaptability	capable of getting accustomed to both external pressure, and in-house breakdown
4	intelligent	Must be dynamic (adapt to the network operator needs)

As mentioned before, SON functions are classified into: i) Self-configuration, Self-optimization and Self-healing networks. Usually network operators utilize skilled humans for detecting, identifying and recuperate the network from whichever outages and failures. The standard framework for fault management is defined by 3GPP [8].

According to the standard framework, the failures and outages refers to hardware and software failures of nodes, system overloading which result in breakdown of nodes, failure in communication among two nodes, etc. At this point, the node will not function in a normal way resulting to full outage. According to 3GPP specifications, if any fault occurs, an alarm must be generated identifying the nodes and it must be able to tell what type of fault has occurred. The alarm might contain extra information regarding the healing of the system, but it all depends on the manufacturer. For few issues alarm is not generated and it cannot be categorized as faults, and such are called as partial outages. Partial outages may happen when there is a change in environment, or rapid variation in traffic. For solving these issues, network operators were reliant on humans. But after the introduction of 4G, network operators cannot rely on humans for checking the irregularities in the network, since the subscriber base and the network size are growing at a tremendous rate.

Investigation was started by SOCRATES project [9] on how to automate the LTE networks and how will be the impact after automation. SEMAFOUR project [10] was launched recently for developing a combined self-management system especially for Heterogeneous Radio Access Networks (RAN). It also includes solutions for detecting network irregularities, analyzing 4G standards and also for future 5G networks. As the cellular network grows, the physical entity in the network also increases. Hence there will be a proportionate increase in the probability of network irregularities (outages). To act to these irregularities, a 3 stage framework is depicted. Self-healing solutions will utilize this framework. Table II shows the simple framework of self-healing solutions.

S No	Stage	Self-healing solutions
1	First - Detecting Network Outages	i) Detecting both partial and full outages ii) If outage detected – outage detection solution flags for additional action
2	Second - Diagnostic Algorithms	i) identify the accurate reason of network outage
3	Third – Outage Compensation	i)give provisional coverage to affected customers

3. Key Components

Self-healing methods comprises of five key components, which are very much useful for the complete development of the work related to self-healing of Mobile Cellular Networks (MCNs). The key components are shown in the following figure 3.

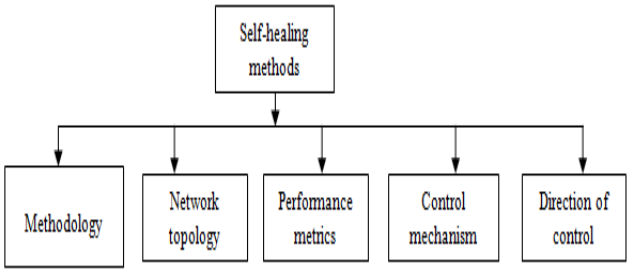

Fig 3 Key components of Self-healing methods

A. Methodology

One of the following three methodologies [Heuristic, learning based and Analytical] must be followed while presenting a solution for the detecting and diagnosing outages. Table III outlines the three methodologies.

Table – III Three Methodologies

S No.	Heuristic	Analytical	learning based
1	a set of pre-defined rules are followed	Problems are broken into mathematical components.	Machine learning techniques
2	Two Heuristic solutions i) rule based – follow of- else rules ii) frameworks – consists of guidelines	Techniques used - Convex and non-convex optimization - game theory - multi-objective optimization	Three types - supervised - unsupervised - reinforcement learning

B. Network Topology

Network topology refers to cell deployment and also it explains the layered network structure. Two types of topologies are used: Homogeneous and Heterogeneous networks. Table IV summarizes the two types of topologies.

Table – IV Two topologies

S No.	Homogeneous	Heterogeneous
1	Only one tier of cells	Macro and Small cells [HetNet]
2	Macro cells - have large coverage area Small cells - have low power and coverage	- Flexible - potential for 5G [11]

C. Performance Metrics

For evaluating the performance of the network, performance metrics are used. These metrics can be got from the entities of the network and the reports generated by the user. In self-healing the performance metrics are coming under the category *network health*. This network health is defined as the term mainly used for explaining the network performance in terms of three [Accessibility, Retainability, Mobility] Key Performance Indicators (KPIs) [12]. The following table V explains the three KPIs.

Table - V Three KPIS

S No.	Accessibility	Retainability	Mobility
1	Network resources are accessed by subscribers for transmission of data	Complete the data session without any drop in data	Subscribers are permitted to change from one cell to another without affecting the services
2	KPIs in terms of success rate - attach, -radio resource control setup, - connection setup , -random access, etc.	KPI - Session drop rate	KPIs - handover attempt, - Success rate - failure rate

In addition, the network coverage also depends on few more signifying measurements, which comprises Signal to Noise Ratio (SINR), Reference Signal Received Power (RSRP), Reference Signal Received Quality (RSRQ), data latency, etc.,. These measurements are utilized while the self-healing solutions are designed and analyzed.

D. Control Mechanism

This method is mainly for controlling the functionality of SON solution and is classified as flows: i) Centralized, ii) Distributed, and iii) Hybrid. The following table VI explains the three methods

Table- VI Three Methods

S No.	Centralized	Distributed	Hybrid
1	A central controller controls the SON functions connected to all nodes	SON functions exist inside the network	- Combination of Centralized and Distributed. - Few SON functions reside in Centralized controller, and rest in Distributed one.

E. Direction of Control

It defines the following: The SON function designed, whether it will optimize the links i) node-to-user, ii) user-to-node, iii) or both. The below table VII gives the solutions designed for the above three links.

Table VII Solutions For The Three Links

S No.	node-to-user	user-to-node	both
1	downlink controlled	uplink controlled	bidirectional control of network in performance

The objective of self-healing is to build resilient network [13] –[16]. Anomalies are to be detected and analyzed, and a self-healing function must be applied to that. See that the self-healing functions must be able to detected any kind of unpredicted changes and actions, and they must react to those changes in a must fast manner. The main function of self-healing is just to monitor the indication of a fault. But the cause of it is not known experimentally. So the self-healing process is considered as a complex one, and is highlighted in the mobile networks which are heterogenous in nature. Very rarely dissimilar fault happens and with these rare cases it is difficult to collect the statistical data for all cases. It is very difficult to find out the root cause of the fault with the collected statistical data. Hence one has to go for machine learning and better methods for finding out the exact cause of the fault.

4. Resilience

The ability of a system to get better or recover after any failure is said to be resilience [17]. But it is different from robustness. At present in complex network, resilience is becoming significant and a challenging one in handling of failures [both internal and external]. These failures may cause total damage of the network. Failures cannot be averted in the networks, and once any failure occurs, the system must be able to survive the failures, are said to be resilience. The behaviour of these networks was examined from various angles by the researchers. It must be noted down here that, one must design the network topologies in such a way that it provides resilience if any failure occurs in the link. A network is said to be a survivable network if it has superior resilience properties. There are lot of potential measures of resilience. Based on the amount of data flow, the resilience of complex network is measured [18]. In complex network resilience (CNR), topological parameters or metrics are considered for the measurement of CNR. Several studies have been made by few researchers regarding the behaviour of these parameters after an attack in the complex network. Two parameters are considered: i) scale of network, and ii) network efficiency. Resilience is not only popular in the field of computer science. It is also admired in the disciplines like management science, environmental science, physcology, etc [19]. Resilience takes two forms with its multidisciplinary nature such as: i) static, and ii) dynamic [20] –[23].

Resilience while static is capable of taking in any fault and immediately will rebound to the original condition, without disturbing the main functions. When dynamic the system will try to move towards a constructive state.

Since everyone is depending on computer, disrupting the network is increasing day by day. The attackers mainly attack the Internet since it is the attraction of people. Hence we observe that resilience is very critical for the future networks and also survivability. To improve both, Resilient and Survivable networks (ResiliNets) are very important [24]. ResiliNets uses a formula as shown in (1).

$$D^2R^2+DR \text{ -- > Resilience} \quad (1)$$

where

D = Defend
D = Detect
R = Remediate
R = Recover
} For Real-time control loop

D = Diagnose
R = Refine
} For System Enhancement

D^2R^2 forms the inner loop and DR is the outer loop. The inner loop happens at real time and is explained as follows. Defend - The network must be in a position to defend itself from any kinds of attack or natural disasters. Detect - Even if all protection is done to the network systems, let us assume that some attack or challenge to the network will happen. At that time the ResiliNets must automatically detect any adverse attack or event occur. Remediate - The impact of the attack must be made minimum once it detects an attack or challenge. Recover - The network must be capable of returning back to its original and regular operations after an attack is over. ResiliNets framework is shown in figure 4.

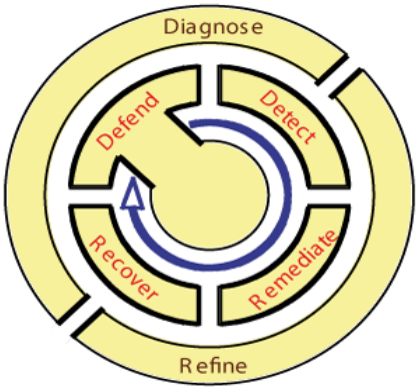

Fig 4 Framework of ResiliNets [25]

The outer loop performs the back ground operations. **Diagnose** – The fault must be immediately diagnosed. The faults must be eliminated or fault tolerance must be added to avoid this kind of malfunction in the near future. **Refine** – Improved in the network must be done. All the strategies must be leaned and it must be improved so that the network resilience is boosted [26]. Table VIII gives the design principles of ResiliNets.

Table VIII ResilNets Design Principles

S No	Categories	Principle
1	prerequisites	i) service requirements ii) normal behaviour iii) threat and challenge models iv) metrics v) heterogeneity
2	tradeoffs	i) resource tradeoffs ii) complexity iii) state management
3	enablers	i) self-protection ii) connectivity iii) redundancy iv) diversity v) multilevel vi) context awareness vii) translucency
4	behaviour	i)Self-organizing and autonomic ii) adaptable iii) evolvable

A. Metrics of Resilience

Recently many authors are writing about resilience, and their importance is ever increasing day by day [27]. An example of how the network behaves before fault or disruption occurs, during and after the situation is portrayed in figure 1. Initially this behavior was presented by [28]. Then on this was fine tuned by [29] - [31]. From figure 1, it is learnt that the network behaves as follows. The network initially is operating in original state S_0 until a disruption d_s happen at time t_1. The maximum the network gets disrupted is at time t_2. The network starts recovering from time t_3. Finally the recovered state S_f is attained at time t_4, and it keeps maintaining it. The network performance is measured as m(t). Thus from the figure 4 it is observed that the performance of the network m(t) is decreasing.

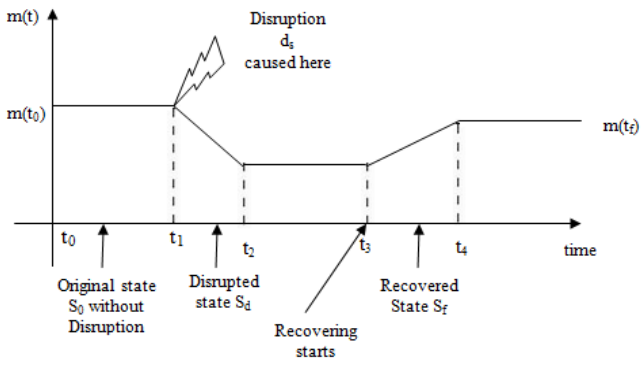

Fig 4. Network Behavior

Resilience is divided into three dimensions as: i) reliability, ii) vulnerability, and iii) recoverability as shown in figure 5. Reliability refers to the capacity of the network to fulfill the expectations of the network.

Vulnerability is the amount of damage caused to the network for a particular trouble. Recoverability is the capability of the network to recuperate after any fault.

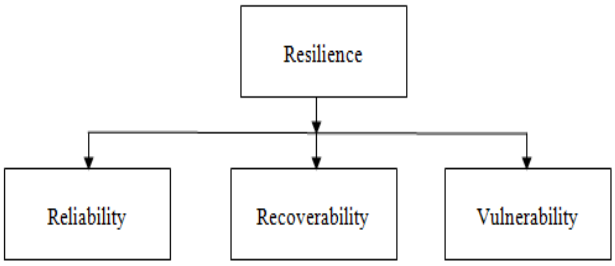

Fig 5. Dimensions of Resilience

5. Self-Healing solutions for future 5G services

5G mobile network will be having a lot of services combined in it. The services include data services, Internet of Things (IoT), legacy call, etc. The above mentioned services will have their own constraints. For example, while providing a wireless connection two important things must be considered: i) data security and ii) robustness [32]. Apart from these two, data rates must also be considered. In the existing scenario, the authors have addressed only legacy issues in self-healing. For example: the call connectivity or transmission of data will be restored if any outage occurs. But they have not addressed other services related to 5G networks. Research is still open for the self-healing services related to IoTs and is considered to be the main challenge [33]. The performance level is different for various services and it is very hard to solve the problems with solution using unified self-healing. However it is considered as a possible solution for solving any outage caused.

6. CONCLUSION AND FUTURE WORK

The most important component in SON is self-healing, since it reduces the Operational Expenses (OPEX) of the mobile network, particularly for future networks. But till now, for cellular networks, a complete study has not been carried out on the existing self-healing techniques. In future, self-healing solutions has to overcome outages which are caused in the forthcoming 5G networks. Lot of research challenges are left out in 5G mobile networks for future work. Possible solutions like unified self healing were discussed for future work, so that the existing research limitations can be addressed.

ACKNOWLEDGEMENTS

The authors acknowledge the support and encouragement given by the Management, Principal, Director of Computer Applications department and Head, Department of Electronics and Communication Engineering, towards this work

REFERENCES

1. Ahmad Asghar, Hasan Farooq, AliImran, “Self-Healing in Emerging Cellular Networks: Review, Challenges, and Research Directions”, IEEE Communications Surveys & Tutorials, Vol. 20, No. 3, 2018
2. “Evolved universal terrestrial radio access network (E-UTRAN); self-configuring and self-optimizing network (SON) use cases and solutions,” 3GPP, Sophia Antipolis, France, Rep. TR 36.902-V9.3.1, 2011.
3. 3GPP, Telecommunication Management; Self-Organizing Networks (SON); Self-Healing Concepts and Requirements, 3GPP Standard TS 32.541-V10.0.0, 2011.
4. A. Gómez-Andrades, P. Muñoz, E. J. Khatib, I. de-la-Bandera, I. Serrano, and R. Barco, “Methodology for the Design and Evaluation of Self-Healing LTE Networks”, IEEE Transactions On Vehicular Technology, Vol. 65, No. 8, 2016
5. P. Donegan, “Mobile Network Outages & Service Degradations: A Heavy Reading Survey Analysis”, Vol. 11, Heavy Reading, New York, NY, USA, Oct. 2013.
6. M. M. S. Marwangi et al., “Challenges and practical implementation of self-organizing networks in LTE/LTE-Advanced systems,” in Proc. Int. Conf. Inf. Technol. Multimedia (ICIM), Kuala Lumpur, Malaysia, 2011, pp. 1–5
7. A. Imran, A. Zoha, and A. Abu-Dayya, “Challenges in 5G: How to empower SON with big data for enabling 5G,” IEEE Network., Vol. 28, No. 6, 2014, pp. 27–33
8. 3GPP, Telecommunication Management; Fault Management; Part 1: 3G Fault Management Requirements, 3GPP Standard TS 32.111-1-V13.0.0, 2016.
9. L. Schmelz et al., “Self-organization in wireless networks use cases and their interrelation,” in Proc. Wireless World Res. Forum Meeting, vol. 22, 2009, pp. 1–5.
10. R. Litjens *et al.*, “Self-management for Unified Heterogeneous Radio Access Networks,” in Proceedings IEEE 77th Vehicular Technology Conference *(*VTC*)*, 2013, pp. 1–5
11. J. G. Andrews et al., “What will 5G be?” IEEE Journal on Selected Areas in Communications, vol. 32, no. 6, 2014, pp. 1065–1082
12. 3GPP, Telecommunication Management; Key Performance Indicators (KPI) for Evolved Universal Terrestrial Radio Access Network *(EUTRAN):* Definitions, 3GPP Standard TS 32.450-V13.0.0, 2016.
13. Janne Ali-Tolppa, Szilard Kocsis, Benedek Schultz, Levente Bodrog, Marton Kajo, “Self-Healing and Resilience in Future 5G Cognitive Autonomous Networks”, IEEE Conferences, 2018, pp. 1 - 8
14. A. Zolli, A. M. Healy, “Resilience – Why Things Bounce Back”, Headline Publishing Group, 2012.
15. A. Berns, S. Ghosh, "Dissecting Self-* Properties", Third IEEE International Conference on Self-Adaptive and Self-Organizing Systems, 2009, pp 10 – 19
16. S. S. Laster, A. O. Olatunji, "Autonomic Computing: Towards a Self-Healing System", Proceedings of the Spring, 2007
17. A. Zolli, A. M. Healy, “Resilience – Why Things Bounce Back”, Headline Publishing Group, 2012.
18. Qiang Dong, Chong Jin,Ruiying Li, Rui kang, “How does node resilience effect on complex networks?”, IEEE International Conference on Software Quality, Reliability and Security Companion, 2018
19. Ilaria Giannoccaro, Vito Albino, Anand Nair, “Advances on the Resilience of Complex Networks”, Complexity, 2018
20. A. Rose, “Defining and measuring economic resilience to disasters,” Disaster Prevention and Management: An International Journal, vol. 13, no. 4, 2004, pp. 307–314. View at Publisher · View at Google Scholar
21. A. Annarelli and F. Nonino, “Strategic and operational management of organizational resilience: current state of research and future directions,” Omega, vol. 62, 2016, pp. 1–18. View at Publisher · View at Google Scholar
22. C. A. Lengnick-Hall, T. E. Beck, and M. L. Lengnick-Hall, “Developing a capacity for organizational resilience through strategic human resource management,” Human Resource Management Review, vol. 21, no. 3, pp. 243–255, 2011. View at Publisher · View at Google Scholar
23. L. Fraccascia, I. Giannoccaro, and V. Albino, “Rethinking resilience in industrial symbiosis: conceptualization and measurements,” Ecological Economics, vol. 137, 2017, pp. 148–162. View at Publisher · View at Google Scholar
24. David Hutchison, James P G Sterbenz, “ResiliNets: Resilient and Survivable Networks”, ERCIM News, 2009
25. David Hutchison, “A Strategy for Network Resilience”, University of Liverpool, 2014.

26. James P.G. Sterbenz · Egemen K. C¸etinkaya · Mahmood A. Hameed · Abdul Jabbar · Shi Qian · Justin P. Rohrer, "Evaluation of Network Resilience, Survivability, and Disruption Tolerance: Analysis, Topology Generation, Simulation, and Experimentation", Telecommunication Systems, 2011
27. Hosseini, S., Barker, K. & Ramirez-Marquez, J.E., "A Review of Definitions and Measures of System Resilience", Reliability Engineering and System Safety, 145, 2016, pp. 47-61
28. Henry, D. & Ramirez-Marquez, J.E., "Generic Metrics and Quantitative Approaches for System Resilience as a Function of Time", Reliability Engineering and System Safety, Vol. 99, 2012, pp. 114-122
29. Barker, K., Ramirez-Marquez, J.E. & Rocco, C.M., "Resilience-Based Network Component Importance Measures", Reliability Engineering and System Safety, Vol. 117, No. 1, 2013, pp 89-97
30. Pant, R., Barker, K., Ramirez-Marquez, J.E. & Rocco, C.M., "Stochastic Measures of Resilience and their Application to Container Terminals", Computers and Industrial Engineering, vol. 70, No. 1, 2014, pp 183-194.
31. Baroud, H., J.E. Ramirez-Marquez, J.E., Barker, K. & Rocco, C.M. "Stochastic Measures of Network Resilience: Applications to Waterway Commodity Flows", Risk Analysis, Vol. 34, No.7, 2014, pp 1317-1335
32. A. Qaddus and A. A. Minhas, "Wireless communication a sustainable solution for future smart grid networks," in Proceedings International Conference Open Source Syst. Technol. (ICOSST), Lahore, Pakistan, 2016, pp. 13–17.
33. J. A. Stankovic, "Research directions for the Internet of Things," IEEE Internet Things Journal, vol. 1, no. 1, 2014, pp. 3–9

AUTHORS PROFILE

Navin Dhinnesh ADC has completed his B.E (ECE) from Madurai Kamaraj University, M.E(CSE) from Anna University, and currently pursuing his Ph.D. He has published lot of papers in International Journals and conferences. His area of research is wireless sensor networks. He is a life member of IETE, ISTE and CSI.

Sabapathi T has completed his B.E (ECE) from Madurai Kamaraj University, M.E(CSE) from Anna University, and obtained his Ph.D in Optical Communication. He has published lot of papers in International Journals and conferences. His area of research is optical communication. He is a life member of IETE, and ISTE.