POLITECNICO DI TORINO

Master's Degree in Communications and Computer Networks Engineering

Master's Thesis

Log Analysis for Event Detection Through Internet over Satellite and Broadband Services

Advisor:
Prof. Roberto Garello
Candidate:
Farzad Aroudi

September 2020

Dedication

This thesis is dedicated to my parents and brother for their love, endless support, and encouragement.

Acknowledgements

Foremost, I would like to express my sincere gratitude to my Professor Roberto Garello for the given opportunity of performing my thesis under his supervision, for his continuous support, motivation, useful comments, remarks, and immense knowledge. His excellence guidance helped me in all the time of writing of thesis.

I would also like to thank all Broadband team colleagues at Skylogic Italia company that supported and trained me during the time I was working on my thesis. Plus, a thank to the RF team for their support.

A special thanks to my family for supporting me spiritually throughout my life.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ASN-GW	Access service network gateway
APSK	Amplitude and phase shift keying
ADSL	Asymmetric digital subscriber line
ATCA	Advanced telecommunication computing architecture
BDC	Block down converter
BEM	Bandwidth efficient modulation
BUC	Block down converter
BSS	Broadcasting satellite service
BPSK	Binary phase shift keying
CP	Circular polarization
CN	Core network
CPE	Customer premise equipment
CMFT	Common mode frequency tracking
DSL	Digital subscriber line
DHCP	Dynamic host configuration protocol
EIRP	Effective isotropic radiated power
FSK	Frequency-shift keying
FLC	Forward link channel
FSS	Fixed satellite service
GEO	Geostationary orbit
GUI	Graphical user interface
HTS	High throughput satellite
HPA	High power amplifier
ITU	International telecommunication union
IF	Intermediate frequency
IFL	Intra facility cable
IoT	Intern of Things
IT	Information technology
KPI	Key performance indicator
LEO	Low Earth orbit
LP	Linear polarization
LNB	Low noise block
LHCP	Left-hand circular polarization
LNA	Low Nosie amplifier
LO	Local Oscillator
LTE	Long term evolution
M2M	Machine to machine

MSS	Mobile satellite service
MAC	Medium access control
MEO	Medium Earth orbit
MPSS	Mac processing subsystem
MIB	Management information base
MM	Mobility manager
MT	Mobile terminal
NMS	Network management station
NDR	Navigation data report
NOC	Network operation center
PSK	Phase shift keying
PEP	Performance enhancing proxies
QoS	Quality of service
QAM	Quadrature amplitude modulation
QPSK	Quadrature phase shift keying
RHCP	Right-hand circular polarization
RL	Return link
RCG	Return channel group
RF	Radio frequency
RRM	Radio resource management
SMTS	Satellite modem termination system
SPL	Search processing language
SNMP	Simple network management protocol
TRIA	Transmit and receive integrated assembly
TTC&M	Telemetry, racking, command monitoring
TWT	Travelling wave tube
TWTA	Travelling wave tube amplifier
TDMA	Time division multiple access
UT	User terminal
UPC	Up power control

Abstract

Nowadays, satellites play an important role to improve life in today's digital economy needs and several industries relies on satellite technology somehow. Moreover, satellites help to save lives in emergency conditions. The entire types of operational satellites are enabling a range of solutions from digital financial services to improve healthcare to smarter cities. Since satellite technologies are more diverse and pervasive but they entirely depend on the radio frequencies availability which can be operated free from remarkable interference. Day-by-day, the global demand for broadband communications increases, and is not limited to a specific location. Thus, providing broadband services is an alternative for those who do not have the access to a maintenance broadband infrastructure in fixed or mobility situation.

One of the most important broadband services is the broadband Internet connection which is provided via satellites and it is also used widely in particular to bridge the digital dividing various areas such as urban and rural communities in order to make high-speed connections available to all users in each region. Following that, well-equipped infrastructure is used to improve and guarantee higher customer service satisfaction as per the service-level agreements. Due to limitations in today's Internet connectivity, 5G mobile Internets is proposed to employ in the future to obtain much higher bit rates in order to provide affordable high-speed Internet connectivity up to 100 Mbit/s per user. Bringing these improvements, satellites will cover large geographical area around the world. Furthermore, all satellite transmitters and aerials for mobility services will be available; beaming up contributions to satellites in Ka-band, where High Throughput Satellites (HTSs) will be available. There would also be limitations such as being costly facilities and the satellite links may be subjected to rain fading. As we move forward, next generation satellites will evolve in various areas including dynamic reallocation of resources, high gain spot beams, and reducing the cost per bit. Consequently, next generation satellites mean IP everywhere, anywhere and have been distinct evolutions, provide global coverage to disperse regions with high data rates, and continue to innovate and offer cost-effective solutions.

Regarding the discussed broadband services and technologies in which the attention is focused on KA-SAT HTS, the important and remarkable point that must be considered is the management and technical support of various areas such as network and systems operations and satellite access network for broadband fixed and mobility data and video services through the infrastructure. All the mentioned areas are involved in technical tasks and activities which are including the monitoring, managing, operating maintenance, and performing troubleshooting operations in critical situations. All these activities and operations will be subjected remarkably to perform immediate actions whenever an incident, anomaly, or any failure is triggered in the KA-SAT platform due to a specific reason in various devices or system components. Considering this, by providing periodic reports, doing periodic health checks for system performance and services, and using professional software and monitoring tools, the relevant platform will work properly and resulting this, provide broadband services with high quality. Consequently, discovering, verifying, and investigating for the root cause of any triggered issue through the KA-SAT platform will have

great importance in applying technical analysis for event detection to improve troubleshooting efficiency.

This thesis will design, develop, and evaluate a log analysis method for event detection as a dashboard with log transaction at both KA-SAT fixed and mobility services in order to identify effectively the occurred anomalies aiming to assist and simplify the root-cause detection for engineers and this is performed by automating the log analysis for the most relevant occurred, linking the triggered logs to the outcomes. Moreover, this analysis is using the applicability of Splunk expertise software within the context of root cause identification for most common anomalies.

Following this, most common use cases are defined and verified, considering the log transaction for event detection, resulting to boost troubleshooting activities and identify more impressively the anomalies occurring on the platform.

Ideally, actions performed, or anomalies spontaneously occurred on the infrastructure (e.g. component failure) will be matched with monitoring data and service impact (e.g. satellite modems drop) and this will apply to technical investigations both for real-time anomalies and past events.

Part I.

Introduction

1. Introduction

1.1. Problem statement

Satellites are serving as a significant role to provide direct broadband services at high-speed data rate and high-quality to terrestrial and mobile users and various business fields covering rural and remote areas overall the world and this coverage is improving and expanding day-by-day. This bidirectional and reliable satellite internet access is provided where the terrestrial infrastructure is not available.

In recent decades, technology of satellite broadband has advanced considerably by using multi-spot beam approach, high frequency bands, and new modulation technique deployment. This enables important advancements in performance and throughput of the satellites.

Moreover, innovations are introduced and designed to resolve limitations such as network capacity, latency, and others in order to incorporate them into new deployed High Throughput Satellite (HTS) aiming to have an efficient and effective performance through delivering the broadband service. Between satellite operators, there is always a challenge in spectrum use for seeking higher frequency bands to utilize for user capacity demands.

KA-SAT is an HTS generation owned by Eutelsat group comprising highly focused beams and multi-spot Ka-band systems with a very high system capacity with the capability of supporting millions of users by delivering high-speed broadband services. Typically, satellite Internet includes three main principle elements; a geostationary orbit satellite, several Earth stations introduced as gateways which can send Internet data to and from the satellite by emitting radio waves, dish antenna with a transceiver at the terrestrial user's location comprising customer premises equipment (CPE), centralized network operations center (NOC) aiming to monitor the whole systems, and other elements as well.

As an important mission and main goal for KA-SAT organization, monitoring KA-SAT service is a highest priority in order to provide broadband service properly. Therefore, the entire described elements and entities depending on the system type must be monitored continually plus protected actively and these key purposes employed to maintain the service operative and avoid any disruptive issues in delivering service. Considering this, satellite gateway components, entire networking system through various areas such as core networks, data center, backbone network, and customer site equipment must be monitored via specific monitoring tools, applications, and platforms.

Regarding KA-SAT service monitoring as a major task, when an abnormal system behavior referring as an incident or failure occurs in the main platform through an area, this generally results to impact on other elements and produce issues and problems. To introduce some typical issues, service outage which creates massive drops for the users to become offline, low signal

performance which is named as service degradation occurring due to variant reasons and others, are certainly important to detect the anomaly and identification the root cause as an investigation procedure and eventually troubleshoot the occurred anomaly in the KA-SAT platform. In this thesis, the following investigation which is considered as log analysis for event detection carried out by using Splunk expertise monitoring tool. To describe the procedure, firstly Splunk applicability in log analysis is discussed, then the log analysis approach for detecting the event by performing experimental method is explained, eventually by doing investigation and working on KA-SAT platform event use cases as analyzing process, the derived results are shown and expressed as dashboard analysis and visualizations.

1.2. Thesis organizations

Part I: Introduction

CHAPTER 1: INTRODUCTION
This chapter starts by explaining the problem statement, precise issue that the thesis is aiming to address, the main purposes and objectives of the thesis, and underlying research approach to achieve the goals.

Part II: Backgrounds

CHAPTER 2: BACKGROUNDS AND RELATED WORKS

This chapter aims to provide various subjects about satellite communications systems principles as backgrounds and KA-SAT High Throughput Satellite (HTS) system overview and employed SurfBeam®2 technology and its relevant network entry, Mobility manager entity and used handover technique, satellite and 5G integration as related works.

Part III: Descriptive Study

CHAPTER 3: METHODOLOGY

This aim of this chapter to explore Splunk expertise and Nagios tools as cases study, describing use case and relevant techniques used in use case definition concept, log analysis conceptualization and its scope in satellite broadband domain, and dashboard design process.

Part IV: ANALYSIS AND DASHBOARD DESIGN

CHAPTER 4: LOG ANALYSIS FOR EVENT DETECTION USING SPLUNK

This chapter is divided into two major parts, log analysis for event detection using Splunk and experimental method. Firstly, Splunk applicability in log analysis approach is discussed and verified.

CHAPTER 5: EXPERIMENTAL METHOD

In this chapter, an experimentation procedure is introduced in order to verify log analysis approach performed on KA-SAT platform event use cases referring as anomaly occurrence during delivering service, eventually providing results as dashboards analysis and visualizations.

Part V: CONCLUSION

CHAPTER 6: CONCLUSION AND FUTURE WORKS

The goal of this chapter is to present conclusions based on the obtained results presented in chapter IV and proposed future directions to investigate and explore based upon the results derived from this research and explain limitations as well.

Part II.

Background

2. Background and Related Works

This chapter is aiming to discuss about various subjects comprehensively including relevant background and related works which are going to be used in the thesis.

2.1. Satellite Communication Systems Principals

This section describes the principles of the satellite communication systems and underlying important fundamentals. It aims to introduce and explain the principal subjects and various elements of a satellite communication system. Firstly, variant basics of satellite systems and communications including typical orbital use, various subsystems, frequency bands use, digital modulations, transmitter and receiver systems, transmission link propagation basis, and RF link are discussed. Afterwards, major subjects comprising high throughput satellite (HTS), satellite and 5G integration, KA-SAT system infrastructure, and handover algorithms are introduced and expressed completely.

2.1.1. Overview

Presently, satellite communication systems are considered importantly as an integral part of wide area telecommunication network all over the world. A complete understanding of satellite system needs to cover variant relevant topics. Moreover, satellite communication networks are taken into consideration as an essential part of most major communication systems. Satellites contain a unique capability of providing coverage over very large geographical zones. These results to provide the connectivity among various communication sources which implies certain advantages in variant applications such as connecting large traffic nodes, end-to-end in direct connections provision to the users, mobile broadband communications, and broadcasting services directly to the public as well. These advantages have made possible this technology to grow in recent decades. Mainly, the most telecommunication benefits have been obtained for point-to-point communication through the domestic and international systems, television broadcast and mobile communications via satellites. Basically, a communication satellite is an electronic communication package possessing various subsystems located in orbit which the main purpose is to initiate the communication data transmission or any messages from one source point to another destination point through the space. The data type transferred mostly often corresponds to voice, video, and digital data. Typically, the communication involves the transmission between a source point and a user point and vice versa. Typically, data transmission operation made through terrestrial media, wire line, coaxial cables, optical fibers, or a combination of these transmission facilities. As described, satellite networks can be radio communication systems aiming to support terrestrial networks to provide services in any requirement case. Following this, by introducing satellite Internet, which is referred as a network of networks, is revolutionizing how information can be accessed and also how users can communicate. By developing the technology through this field

combined with new network architectures interconnecting variant information systems made properly an information infrastructure globally. Subject to this, many broadband applications and services aiming to deliver to the residential and enterprise users with respect to the high bandwidth demands and quality of service guarantee. The result of this demand is to employing multiple access technologies via ranging from various transmission facilities line to cable, digital subscriber line (DSL), wireless and satellite as well. Consequently, satellite communication has an importance role through supporting access to the Internet over a satellite network infrastructure. From a technical standpoint, a satellite communication network is specified by specific attributes such as broadcasting capability, reliability, global coverage, scalability, and flexibility of bandwidth- on-demand.

2.1.2. Satellite Orbits

The locations of the orbits through the spacecrafts in a communications satellite system play an important role in determining the coverage and operational features of the services delivered by that system. This section aims to discuss about the typical attributes of satellite orbits and consider summarily the features of the most known orbits for communication applications. The determination of the satellite orbits is according to the motion laws and mechanics and gravitation laws as well. The forces act applied on the satellite in which the gravity pulls the satellite in toward the Earth, while the orbital velocity of the satellite pulls it away from the Earth. Considering this subject, the gravitational force F_{in}, and the angular velocity force,F_{out} in which $F_{in} = F_{out}$ is shown as following formulas: [1]

$$F_{in} = m \times \frac{\mu}{r^2} \quad \text{and} \quad F_{out} = m \times \frac{v^2}{r} \quad \text{and} \quad v = \frac{\mu^2}{r^2}$$

Where,
m = satellite mass
v = satellite velocity
r = distance from the center of the Earth which is referred as orbit radius
μ =Kepler's Constant =$3.986004 \times 10^5\ km^3/S^2$

Kepler's Laws Concepts

In space, the Kepler's laws of planetary motion enforce to any bodies which interact through the gravitation. The motion laws are described into three basic principles which explained in following paragraphs and all the Kepler's laws are illustrated in figure 2.1.
Kepler's First Law which applies to artificial satellite orbits and stated as the path followed by a satellite around the Earth at which is an ellipse shape, including the center mass of Earth which considered as one of the two foci of the ellipse.
Kepler's Second Law can be similarly described as equal time intervals which the satellite sweeps out equal areas within the orbital plane.
Kepler's Third Law is the square of the periodic time of orbit which is proportional to the cube of the mean distance at which the formula is presented in following: [1]

$$T^2 = \frac{4\pi^2}{\mu} a^3$$

Where:

T = orbital period, in s
a = distance between the two bodies, in km
μ =Kepler's constant = 3.986004 × 105 km3/s2

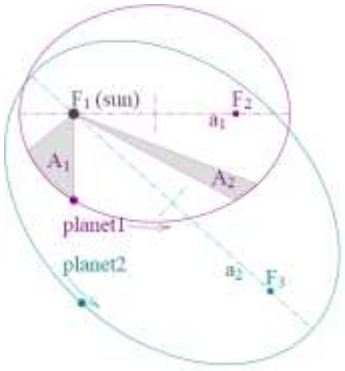


Figure 2.1: Kepler's three laws with two planetary orbits illustration [2]

Orbital Parameters

According to the figure 2.2, which shows two perspectives which is useful in stating the significant orbital parameters used to explain the characteristics of Earth-orbiting satellite. The important parameters are defined as the following items: [1]

- **Apogee**: It is the point which is the farthest distance from the Earth.
- **Perigee:** It is the point which is the closest approach to the Earth.
- **Line of apsides**: The line which joins the perigee and apogee points through the center of the Earth.
- **Ascending node**: The point where the orbit crosses the equatorial plane which is crossing from south to north points.
- **Descending node**: Like the previous node, it is the point where the orbit crosses the equatorial plane, which is crossing from north to south points.
- **Line of nodes**: The line which joins the ascending and descending nodes through the center of the Earth.
- **Argument of perigee, ω**: Introduced as an angle form ascending node to perigee which is measured in the orbital plane.
- **Right ascension of the ascending node side, φ**: Defined as an angle which is measured in eastward, through the equatorial plane, starting from the line to the first point of Aries (Y) to the ascending node.
- **Eccentricity**: Described as a measure of the "circularity" of the orbit. It is determined by the following formula:

$$e = \frac{r_a - r_p}{r_a + r_p}$$

Where
e = the eccentricity of the orbit
r_a = the distance from the center of the Earth to the apogee point
r_p = the distance from the center of the Earth to the perigee point

- **Inclination angle**, θi: It is the angle placed between the orbital plane and the equatorial plane of the Earth.

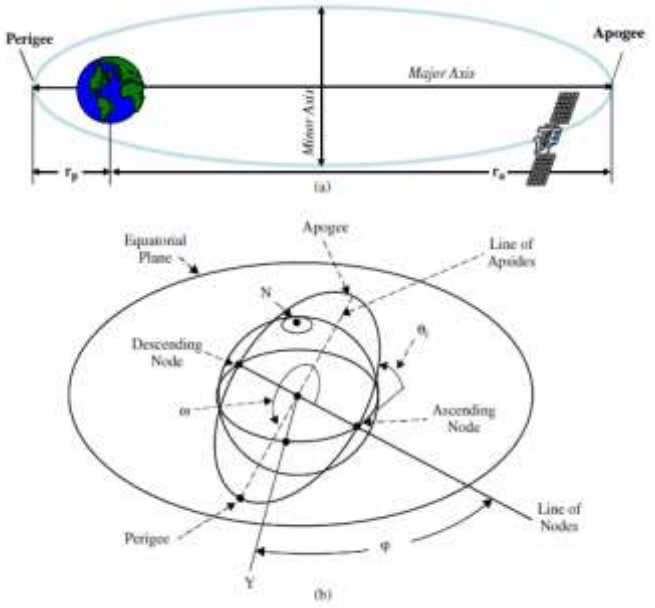


Figure 2.2: Illustration of Earth-orbiting satellite parameters [1]

Regarding the entire described parameters available to the satellite designer, there are a certain list of possible orbits that can be used commonly for communications, sensor, and scientific satellites. The most known orbit which is used for communication satellites is the geostationary or geosynchronous orbit. As implied, the most of the first-generation satellite systems used geostationary (GEO) whereas next generation satellite networks comprise medium Earth orbit (MEO), low Earth orbit (LEO), or some combinations of these configurations. In the following, common types of satellite Earth orbits are described in detail respectively in the following items:

Geostationary Earth Orbit (GEO)

The altitude in GEO satellites is around 35,000 km above the Earth's surface and the orbit period is 24 hours which provide the continuous visibility and fixed geometry. This approach is one of the major distributions means of television, telephone, and data communications throughout the world. Currently, the most commercial telecommunications satellites which are in operation are placed in GEO orbit. In this case, a satellite can cover about one third of the surface of the Earth and this is the most capability of GEO satellites. The GEO orbit is shown in figure 2.3. [3]

Medium Earth Orbit (MEO)

In this orbit, the satellites operate in the range between LEO and GEO orbits, typically at altitudes of 10,000 to 20,000 km. The MEO orbit is shown in figure 2.3. To imply the characteristics of the MEO orbit, they include repeatable ground traces for recurring ground coverage, selectable number of revolutions per day and motion of relative satellite-Earth for allowing to measure the accurate and precise position. A common MEO one would provide one to two hours of observation time for an Earth terminal at a fixed location. MEO satellites have features to be employed for various applications such as meteorological, remote sensing, navigation, and position determination applications. [1]

Low Earth Orbit (LEO)

The altitude of LEO satellites is generally between 700 and 2000 km and in near circular orbits. The orbit period is between 100 to 120 minutes. The low Earth orbit satellite includes certain features that can be advantageous for communications applications which is shown in figure 2.3. To imply these features, the Earth-satellite links are much shorter, leading to lower path losses resulting lower power, and contains smaller antenna systems. Furthermore, the propagation delay is less due to shorter path distances. LEO satellites, with the appropriate inclinations can cover high latitude locations, including polar areas, which this cannot be reached by GEO satellites. [1]

Figure 2.3: Earth Satellite Orbits

2.1.3. Satellite Subsystems

A communication satellite system includes major segments, space, and ground segments, starting from an orbital configuration of space to ground components and network elements as well. The specific satellite system application such as fixed, mobile, and broadcast satellite service, will determine the system elements. The principle system comprises a satellite in space, relaying information among the user terminals through Earth stations and the satellite. The information of the user is required to be transmitted via terrestrial devices to connect with the ground terminals. The control of the satellite is managed by a satellite control facility located on the ground in which referred as master control center handling various functions such as tracking, telemetry, command, and monitoring.

The Space Segment includes the orbiting one or more satellites and the ground satellite control keeps the satellites operational and the ground segment includes the transmit and receive Earth stations and the relevant equipment to interface with the user. Both segments are described as following: [1]

Space Segment

This segment is classified into two operational areas, the bus and the payload which are shown on Figure 2.4. The bus is described as a principle satellite structure and the subsystems which supports the satellite as well. The bus subsystems include the physical structure, power, attitude and orbital control subsystem, thermal control subsystem, and command and telemetry subsystem.

The payload is the equipment that provides the service. It includes the communication equipment which provides the relay link between the uplink and downlink from the ground. Furthermore, the payload is divided into subsystems of transponder and the antenna. Both elements are described in following paragraphs. [1]

Figure 2.4: Illustration of communications satellite subsystems [1]

- **Satellite Bus**

According the shown figure2.4, the satellite bus system made from various subsystems which include physical structure, power subsystem, attitude and orbital control, and tracking, telemetry, command, and monitoring (TTC & M) subsystems.

The physical structure of the satellite is considered as a centralized home location for the whole components of the satellite. The basic structure depends on the employed stabilization method to keep the satellite stable and pointing in the intended direction, means to keep the antennas oriented toward Earth correctly.

The power subsystem is the electrical power to operate the equipment on a communication satellite which is supplied from solar cells, which convert incident sunlight into electrical energy.

The attitude control of a satellite is considered as the satellite orientation through space regarding the Earth. Attitude control is necessary to apply so that the antennas, which typically have narrow directional beams, are pointed properly towards Earth. The orbital control is the process to maintain a satellite in its correct orbit location.

The thermal control system controls the large thermal gradients generated in the satellite by removing or relocating the heat to deliver stability in temperature environment in the satellite.

The subsystem of tracking, telemetry, command, and monitoring (TTC&M) subsystem delivers necessary spacecraft management and control functionalities to maintain the satellite operating in a safe status in the orbit. The transmission links relating to this subsystem among the satellite and the ground are separate from the links of communication systems. Figure 2.5 depicts the typical elements for the satellite and the ground facilities. This subsystem comprises the antenna, command receiver, tracking and telemetry transmitter. Telemetry data which typically includes the payload and power attitude control is received by other subsystems. The command data is relayed via command receiver to control the parameters such as antenna pointing, transponder, battery etc. Monitoring and controlling of the satellite are performed through monitor and keyboard interface automatically.

Tracking determines the current orbit, position, and movement of the spacecraft. The telemetry role collects the data from sensors on-board the spacecraft and then relay them to the ground. The command complements the telemetry role. It is responsible for relying specific control and operations information from the ground to the spacecraft. [1]

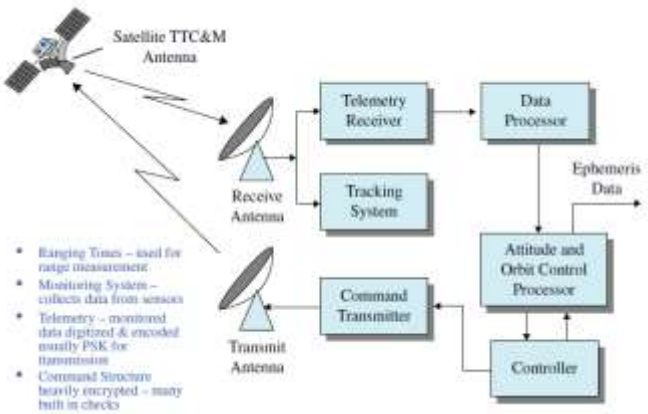


Figure 2.5: Illustration of tracking, telemetry, command, and monitoring unit [1]

- **Satellite Payload**

The leading elements of the payload segments, particularly for communications satellite systems are the transponder and antenna subsystems.

The transponder includes the series of components that provide the communications channel, or link among the uplink signal which is received at the uplink antenna, and the downlink signal which is transmitted by the downlink antenna. Generally, each transponder operates in a various frequency band. A typical design typically can accommodate a certain number of transponders that each one has a definite bandwidth. A typical commercial communication satellite can accommodate among 24 to 48 transponders, operating in various bands such as C-band, Ku-band, or Ka-band.

The transponder numbers can be augmented using polarization frequency reuse, where two carriers at the same frequency bands, but with orthogonal polarization means, linear polarizations (horizontal and vertical), or circular polarization, (right-hand and left-hand) are used. The satellite transponder is typically implemented in one of two configuration types which are the frequency translation transponder referred as bent pipe and the on-board processing transponder.

In the first type, the frequency translation transponder receives the uplink signal, amplifies, and retransmits it with a translation in carrier frequency. Figure 2.6 shows the typical implementation of this type in which the uplink radio frequency is converted to an intermediate lower frequency, amplified, then converted back up to the downlink RF frequency to transmit to the Earth. [1]

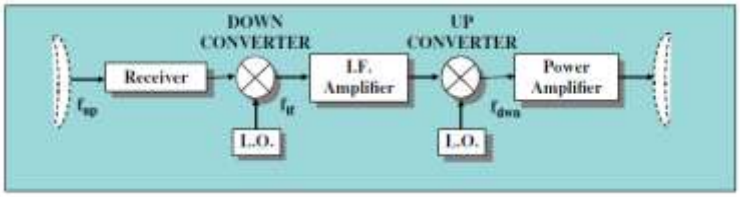


Figure 2.6: Frequency translation transponder [1]

Figure 2.7 shows the second type of satellite transponder which is the on-board processing transponder. The uplink signal is demodulated to baseband. The baseband signal is available for processing on-board including reformatting, error-correction, etc. [1].

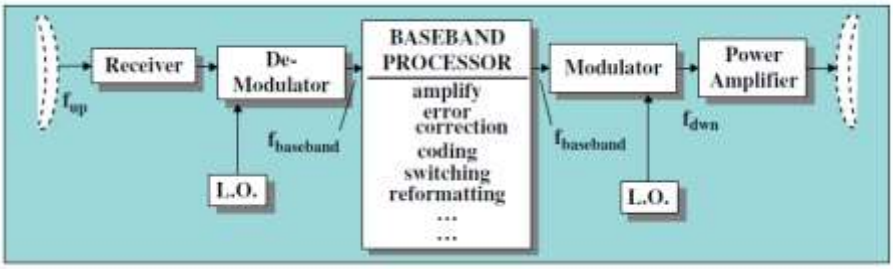


Figure 2.7: Illustration of on-board processing transponder [1]

The demodulation process removes uplink noise and interference from the downlink. Traveling wave tube amplifiers (TWTAs) are utilized to deliver the final output power required for each transponder channel. The TWT is a slow wave structure device, which operates in a vacuum envelope, and requires permanent magnet focusing and high voltage DC power supply support systems.

The antenna systems are used for transmitting and receiving the RF signals which include the space links of the communications channels. The antenna system is a critical part of the satellite communications system to increase the strength of the transmitted or received signal to allow amplification, processing, and eventual retransmission. The most important parameters which define the performance of an antenna are such parameters including gain, beam width, and antenna side lobes. The gain, which is expressed in dBi, defines the incensement in strength obtained in concentrating the radio wave energy at both transmission and reception, by the antenna system.

The beam width is expressed as the half-power beam width which is a measurement of the angle over at which the maximum gain occurs. The side lobes define the gain amount in the off-axis directions. [1]

Ground Segment

Considering the ground segment, which is referred as Earth station, it is component of the satellite network. It delivers functions of transmitting and receiving traffic signals to and from satellites. Moreover, it provides interfaces directly to the user terminals or terrestrial networks. In general, the Earth station includes the transmitting and receiving antenna, low noise amplifier (LNA)s and high-power amplifiers (HPAs), up and down converters, power suppliers, modulation, demodulation and coding, and interfaces to terrestrial networks or user terminal. [4]

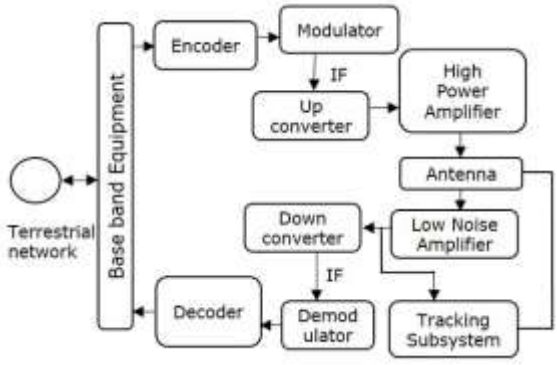


Figure 2.8: Digital Earth station illustration [5]

2.1.4. Satellite Transmission Frequency Bands

Frequency bandwidth is a significant resource of satellite networking. The radio frequency spectrum is ranging from 3 kHz to 300 GHz. The propagation environment between the satellite and Earth station because of various factors such as rain, snow, gas and others and limited satellite power from solar and battery as well limits further bandwidth for the satellite communications. Figure 2.9 represents the attenuations of various frequency bands due to rain, fog and gas factors. [4]

Frequency bandwidths are allocated by the international telecommunication union (ITU). Table 2.1.4 shows the different available allocated bandwidths for satellite communications. [4]

Denomination	Frequency bands (GHz)
UHF	0.3–1.12
L band	1.12–2.6
S band	2.6–3.95
C band	3.95–8.2
X band	8.2–12.4
Ku band	12.4–18
K band	18.0–26.5
Ka band	26.5–40

Table 2.1: Typical frequency bands of satellite communications

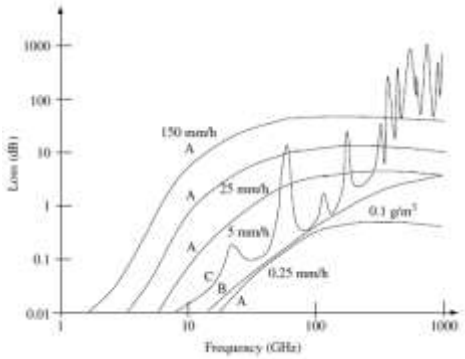


Figure 2.9: Frequency bands attenuations due to A: rain, B: fog and C: gas [4]

In satellite communications, the typical use of the frequency bands is described as following items respectively: [6]

Ku-Band

Ku-band spectrum allocations are more common than C-band which comprising 750 MHz for fixed satellite services and 800 MHz for the broadband satellite services. Generally implemented by various satellites covering variant regions in which Ku spot beams with geographic separation allow up to approximately 10X frequency reuse. The maximum available Ku-band spectrum could be more than 4 THz amount. The more progressive regulations at Ku-band also favor its use for two-way interactive services like voice and data communication. [6]

Ka-Band

Ka-band spectrum is used commonly for services that cannot find room at the lower frequencies. About 2 GHz of uplink and downlink spectrum available allocated on a worldwide basis. The Ka-band region of the spectrum is the last to be exploited for commercial satellite communications. Technically, Ka-band contains much greater attenuation for a given amount of rainfall. The popularity of broadband access to the Internet via DSL and cable modems has encouraged several organizations to consider and use Ka-band as an effective means to reach the individual subscriber. [6]

Q-Band and V-Band

According to these frequency bands, the frequencies above 30 GHz are considered to be experimental in nature and have not been used to fit to exploit this region. The reason is that more intense rain attenuation is existed and even atmospheric absorption that can be experienced on space-ground paths. Moreover, Q-band and V-band are considered as a challenge in terms of the active and passive electronics onboard the satellite and within Earth stations. The dimensions are small, amplifier efficiencies are low, and everything is more expensive to build and test. [6]

2.1.5. Digital Modulations

Digital modulation defines transferring of the bit stream to an RF carrier at which the techniques of QPSK and 16-QAM are used. In this process, the steps comprise generating a bit in the form of a pulse that can meet the required criteria for bandwidth and shaping, then transferring those shaped pulses onto a carrier, generally using form of PSK which allow for impairments, noise, and interference across the transmission link and providing a suitable demodulator capable of recovering the pulses from the carrier to reproduce the digital bit stream with the minimum errors. [6]

Frequency Shift Keying

This digital modulation is used in radio communications. Typically, FSK is achieved by switching between two discrete frequencies in which correspond to the 1 and 0 states, respectively or reversely. This causes FSK to consume more bandwidth of PSK. The advantage use of FSK is that simple hardware can be utilized in the modulator and the demodulator. Today, this modulation is not used due to requiring more signal power for providing the same performance in terms of error. [6]

Phase Shift Keying

This technique is the most typical system used to transmit and receive data with high speed over satellites. Typically, the PSK modems operate at ranging rates from 64 kbps to 1,000 Mbps. Considering BPSK and QPSK techniques, BPSK uses two phase states which are 0 and 180 degrees, and QPSK uses four states split into pairs, 0, 180, 90, and 270 degrees. To imply the advantage of QPSK, it is efficient in the use of bandwidth and power. [6]

Amplitude and Phase Shift Keying

To describe this technique, firstly, the bandwidth efficient modulation (BEM) must be defined as considering a solution to be efficient only in terms of bandwidth and this is accomplished by using more satellite transmitted power or using a larger antenna in Earth station. Regarding this definition, the most typical form of BEM is amplitude and phase shift keying (APSK) which both the phase and amplitude are variable to carry the stream data bits. [6]

2.1.6. Earth-space Transmission Link Propagation

Radio wave propagation is referred as a process in which the radio signals reach the receiving antenna from the transmitting station. In general, the radio waves represent as a portion of the electromagnetic spectrum. The common electromagnetic spectrum part for commercial satellite communications is ranging from 1 to 60 GHz. The figure 2.10 represents the microwave spectrum including satellite bands is used in satellite communications. [6]

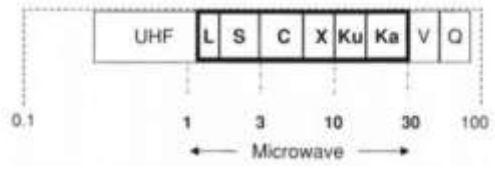


Figure 2.10: Microwave spectrum, including satellite bands [6]

Principal Microwave Propagation

In general, the electromagnetic wave energy propagates out radially. The pattern of spreading reduced in intensity reversely to the square of the distance. In free space, entire radio waves behave in this way, but different forms of matter generate potentially disruptive effects and results when placed through their paths. The reason is related to the microwave energy which can be absorbed,

scattered, bent, and reflected. Thus, there would be additional signal power loss that must be calculated in the satellite link design.

Isotropic Radiator

The isotropic source is the most basic type of radio antenna that is similar to the lightbulb. Generally, at a fixed radius from an isotropic source which is referred as a sphere, the intensity of energy is constant amount. To measure the signal intensity at a specific radius in units of watts per square meter, is calculated by the following formula: [6]

$$P/A = Pt / 4\pi r^2, \quad W/m2$$

Where
Pt = Isotropic source power
$4\pi r^2$ = Sphere area of uniform received energy (Spreading factor)

Polarizations

To describe a property of an electromagnetic wave is called polarization which depends on the angle of rotation of the transmitting antenna. The most common polarization types are linear and circular polarizations. In linear polarization, electrical current from the transmitter flows across the rod first upward and then downward which oscillates at the frequency of transmission. The electrical currents along the rods cause the electromagnetic wave to have its electric component to be lined up through the same direction, which is in vertical direction and is called linear polarization (LP) and divides into two horizontal LP and vertical LP types as well.
Other polarization type is circular polarization (CP). In this polarization, the receiving antenna is not aligned for the transmitting antenna's polarization. Right-hand CP (RCP) and left-hand CP (LCP) are major types of this polarization. [6]

Rain Attenuation

Rain attenuation is the most disruptive effect on commercial satellite links, which results from absorption and scattering of microwave energy by drops of the rain. The signal loss increases with frequency with respect to the various frequency bands. Rain attenuation is not predictable on an instant basis, but by using statistical estimates is feasible to design the links. Intense rain is contained in rain cells, which is limited in terms of geographical size. The rain cell dimensions change according to the rain rate and is measured in millimeters per hour. At a specific rain rate and cell size as well, the attenuation increases through the length of the path within the cell. Figure 2.11 represents the rain attenuation data as a function of frequency and for a temperate climate. [6]

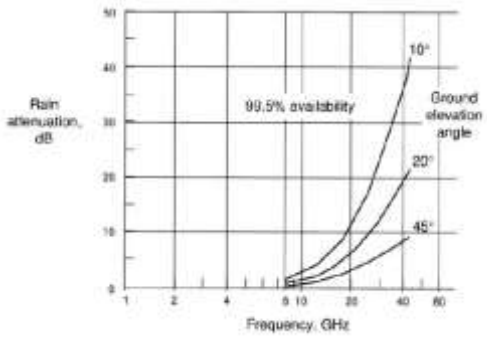


Figure 2.11: Rain attenuation for a temperature climate [6]

2.1.7. Microwave Transmitters and Receivers

The fundamental components in a satellite communication link are represented in Figure 2.12. According to this figure, the transmitting Earth station establishes the uplink path, a satellite and its microwave repeater, the downlink path, and a receiving Earth station.

The points of entry and exit through the propagation medium are delivered by the transmitting and receiving antennas. A transmitting Earth station includes equipment which modulates the data to be transmitted on an RF signal as a carrier signal, then translates it to a proper frequency and finally amplifies it to a high-power level to deliver an uplink path. All these processes are similarly performed for receiving Earth station but inverse direction. [6]

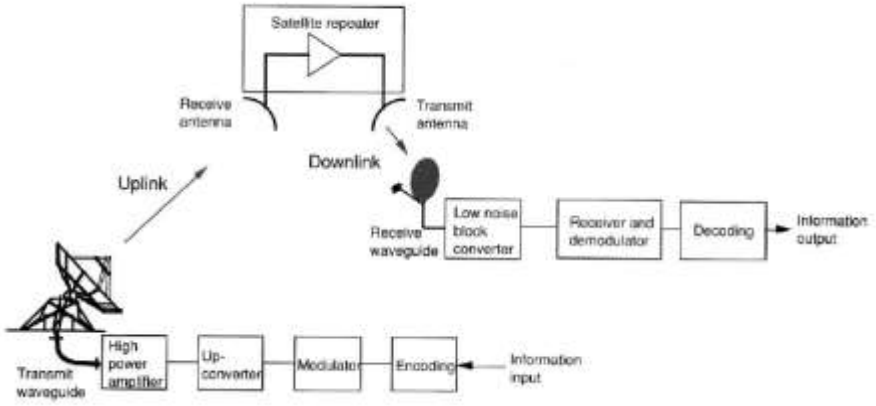


Figure 2.12: Major elements of a satellite transmission link based on end-to-end approach [6]

Transmitting Station

Based on the Figure 2.13, this block diagram represents a single transmitting chain of a typical microwave station, including the signal input at the left side and the RF output departs from the transmitting antenna at the right side. The transmitted signal includes the information in electrical form, such as voice channels for telephone service, digital data in high speed bit stream, and video signals. In modern satellite systems, analog information voice and TV forms are digitized initially, and then compressed to decrease the required bandwidth. [6]

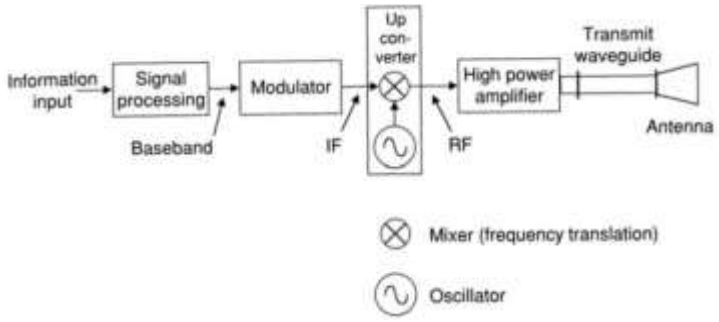


Figure 2.13: Block diagram of a microwave transmitting station and various components [6]

Encoding and Modulation

In this element, the digital information is prepared for transmission over the link path. Encoding includes certain processes which typically match the information data to the specific features of the satellite link. The most common forms of encoding techniques and their applications are described as following items: [6]

- **Forward error correction:** It reduces the error rate. This increases the bit rate of output to accommodate redundant bits. In some cases, this technique is incorporated into the modulation and demodulation roles which are performed by the modem.

- **Compression:** It is responsible for reducing the whole bit count, either lossless or lossy. The benefits would be forwarding less data and provide a better link utilization.

- **Encryption:** This is related to the information security and it is in charge of making data private and difficult to corrupt. With this, the throughput will be more.

- **Protocol adaption:** It deals with data communications networks, generally employing the Internet protocol suite. This improves the user experience in case of facing impairments of satellite link like bit error rate and delay as well.

Consequently, the encoding output is referred as the baseband signal. This baseband signal is taken by modulator to apply it to an RF carrier signal. The inverse process is called demodulation which the baseband is removed from the carrier signal. [6]

Frequency Conversion and RF Amplification

The output of modulator is typically the RF carrier signal, which is not at microwave frequencies typically, but it is centered within a standard frequency channel which is referred as the intermediate frequency (IF). Most common transmitting and receiving stations utilize 70MHz as the IF which it allows to modulators and demodulators to interchange and interconnect by cords and coaxial switches. [6]

High Power Amplification

The final active component is the high-power amplifier (HPA) through the transmitting station. The major function of the HPA is to enhance the microwave carrier power from the low output of the upconverter to the level of power which is required to obtain satisfactory uplink operation. It is required that the HPA contains adequate bandwidth to operate at the allocated microwave frequency. [6]

Receiving Station

As described, the reverse transmitting station process is called receiving station process and it is illustrated in Figure 2.14. Typically, the microwave signal which is received by the receiving antenna is weak and initially it is required to be raised to the power level that can be accommodated by the processing components. This operation is performed by the low-noise amplifier (LNA) in which the gain must meet variant requirements. Other components perform functions that are reverse of transmitting station process. When an integrated downconverter is added to the LNA, the outcome component is named as a low-noise block converter (LNB). [6]

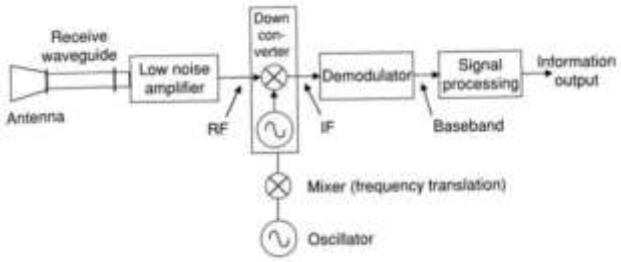


Figure 2.14: Block diagram of a microwave receiving station and various elements [6]

Low Noise Amplifier

The noise is expressed as an equivalent noise temperature in Kelvin (K). The Kelvin scale normally begins at the absolute zero noiseless condition and measures the average random electrons motion energy within the receiver electronics. Thus, the random energy of the electrons is equal to the noise power that overlays the desired signals within the amplifier passband. All LNAs used in satellite communications Earth stations use low noise transistors. The main purpose of this element is to decrease the input loss and amplify a very low power signal with no degradation in signal to noise ratio. [6]

Upconverters and Downconverters

Based on the represented figure 2.15, downconverter and upconverter equipment are responsible for transferring the communication carriers among the operating RF frequencies and the IF which is used by the modems and baseband equipment. A common upconverter includes a primary amplification step to provide enough gain for the operation of station equipment. The frequency conversion is performed by a mixer.

Downconverter and upconverter equipments illustrated in Figure 2.15 (a) and Figure 2.15 (b), respectively, are needed to transfer the communication carriers between the operating RF frequencies and the IF used by the modems and baseband equipment. A typical upconverter has a first stage of amplification to provide adequate gain for the operation of the station equipment. The actual frequency conversion is accomplished in a mixer and local oscillator (LO) combination.

A frequency agile upconverter use a frequency synthesizer to produce the LO, thus any carrier frequency within the satellite uplink band can be employed. In downconverter, the primary amplifier stage delivers the required sufficient gain and mitigate the mixer and IF equipment noise contribution. [6]

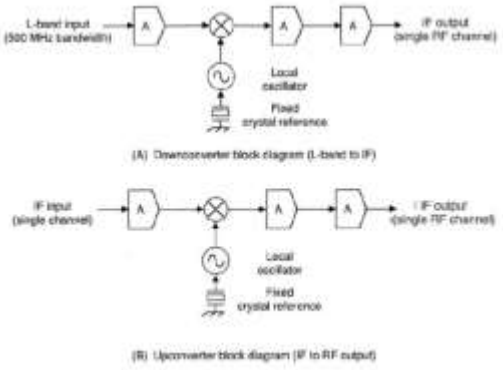


Figure 2.15: Block diagrams of common upconverter and downconverter [6]

Uplink Power Control

To compensate the link fading, certain transmit Earth stations employ automatic uplink power control (UPC) in order to compensate the rain attenuation and other attenuations pertaining to climate. The principle about UPC is the rain-induced fading which is compensated in direct response to the attenuation factor. The uplink entity can be measured accurately only at the satellite. This entity is self-contained and is responsible for adjusting the power of uplink signals to compensate for various weather conditions. [6]

2.1.8 Radio Frequency link

This section aims to introduce the principle elements of the communications satellite radio frequency. According to these elements, the main transmission parameters such as gain of antenna, free-space path loss, and the fundamental link power equation which are considered to determine the RF link performance are described. Moreover, the system noise concept in various parameters which is considered in quantifying on the RF link, is discussed. In the following, the important parameters of link performance are expressed. [1]

Transmission Principles

Since the RF segment of the satellite communication link is critical element that impacts on the design and link performance, the principle parameters of the link must be identified initially

through the basic communication link which is depicted in figure 2.16. These parameters pertaining to the link are described as following items: [1]

P_t = Transmitted power (watts)
P_r = Received power (watts)
g_t = Transmit antenna gain
g_r = Receive antenna gain
r = Path distance (meters)

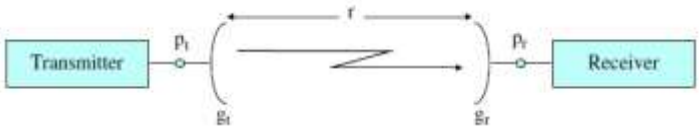


Figure 2.16: Illustration of basic communication link [1]

To introduce the wavelength of the radio wave, it is defined as spatial separation of two successive oscillations referring the distance of travelling the wave during one oscillation cycle. Thus, the frequency and wavelength in free space is defined by: [1]

$$\lambda = \frac{c}{f}$$

with $c = 3 \times 10^8$ m / s

Considering the radio wave propagation in free space from a point source P which is P_t, the wave is radiating spherically from this source point P_t. The power density over the surface of radius r from the implied point P is given by following equation: [1]

$$(pfd)_r = \frac{P_t}{4\pi r^2} \text{ Watts / } m^2$$

Where r is radius, P_t is transmitted power, and pfd is power density. [1]

Following this, the power density can be expressed in dB as:

$$(\mathrm{PFD})_r = 10\log\left(\frac{P_t\, g_t}{4\pi r^2}\right) = 10\log(P_t) + 10\log(g_t) - 20\log(r) - 10\log(4\pi)$$

Where the parameters of P_t, g_t, and effective isotropic radiated power (EIRP) the transmit power, transmit antenna gain, and effective radiated power and all expressed in dB. [1]

To describe an important parameter in the RF link evaluation, effective isotropic radiation (EIRP) is defined as: [1]

$$\mathrm{EIRP} = P_t + g_t$$

The gain of an ideal antenna including a physical aperture A is defined as following: [1]

$$g_{ideal} = \frac{4\pi A}{\lambda^2}$$

Where A and λ are aperture and radio wave wavelength respectively. Besides, the gain can be expressed in dBi as: [1]

$$G = 10\log\left[\eta_A \frac{4\pi A}{\lambda^2}\right], \text{dBi}$$

Considering to spreading loss factor which is a function of wavelength or frequency is defined as: [1]

$$S(\mathrm{dB}) = \frac{\lambda^2}{4\pi}$$

By introducing the spreading loss factor, the free space path loss term can be expressed in dB as: [1]

$$L_{FS}(\mathrm{dB}) = 20\log\left(\frac{4\pi r}{\lambda}\right)$$

To describe the basic link equation for the received power at the receive antenna terminals, it can be determined expressed in dB by following equation: [1]

$$P_r(\text{dB}) = \text{EIRP} + G_r - L_{FS}$$

This outcome provides the basic link equation which is referred as equation of link power budget for a satellite communication link. [1]

System Noise

The service quality is degraded by the noise and interference factors. Interference occurs often due to the RF transmission of another source. Furthermore, the noise is random in nature due to resulting from the random motion of electrons or the receiving equipment or other factors in the environment. White noise is the most typical one on satellite links and produces random voltage fluctuations the noise power density in watts per hertz is equal to the equivalent noise temperature in Kelvins, shown as following: [6]

$$N_0 = k \, . \, T$$

Where, k is Boltzmann's constant.

The noise power which impacts a given signal is that which lies through the bandwidth of the signal means B is as following: [6]

$$N = K. T. B$$

Where B, K, and T are signal bandwidth, Boltzmann's constant, and equivalent noise temperature, respectively. [6]

To introduce an easy method to quantify the noise generated by an amplifier or other device in the communications signal path is noise figure with notation, nf. Typically, the noise figure is defined as: [6]

$$nf = \frac{\frac{p_{in}}{n_{in}}}{\frac{P_{out}}{n_{out}}}$$

Where,

p_{in}, n_{in}: Input power and noise

P_{out}, n_{out}: Output power and noise

To introduce other noise, inside the system at the receiver antenna which generated from the physical antenna structure itself referred as antenna losses produced by the physical structure, and from the radio path which is referred as radio noise which produced from natural and human induced sources. The first one will impact as a reduction on the radio wave power level and the second one will add an increase to the system noise in the antenna temperature of the receiver. [1]

The next parameter which is important to consider is figure of merit which determines the quality of the receiver portions of a satellite communications link. [1]

Link Performance Parameters

To explain one of the problems in designing microwave link is understanding precisely how a specific signal will be impacted by the noise, which is random in nature and by interference from other radio carriers as well.

Regarding the carrier-to-noise ratio, the carrier strength relative to the noise determines the quality of transmission. This is obtained by understanding the power level of the baseband signal from the receiving station's signal element that can be boosted by performing power amplification. Besides this, the noise will be amplified too. The only way to improve the transmission quality is suppressing the noise at receiver input. This is the main reason that the actual link performance is measured by the ratio of RF carrier signal power to noise power. The ratio is represented as following relation: [6]

$$\frac{C}{N} = \frac{E_b}{N_0} \times \frac{R_b}{B}$$

Where R_b is the information bit rate, B is the carrier bandwidth, and E_b is the energy per bit.
The next parameter is the ratio of carrier-to-noise density which is often used in link calculations and is defined as following: [6]

2.2 Related Works

This section aims to present information about the relevant related works such as introducing new generation satellite, satellite and 5G technology integration, KA-SAT platform introduction, and handover technique used in KA-SAT platform.

2.2.1 High Throughput Satellite (HTS)

This section aims to provide a general description about High throughput satellite systems and technology with respect to the various areas in satellite communication filed. Following this, the topics of multiple access schemes and frequency reuse basics, considered by a discussion on the HTS spot beam approach, the operational frequency bands, color patterns, the losses and rain considerations, and some typical application in HTS systems. Finally, approaches on Ka-based and Ku-based HTS systems and comparisons are provided briefly and also an example of commercially deployed HTS is described. [7] [8]

An HTS system can be described as a satellite system that makes possible use many confined spot beams geographically distributed through a specified service area, offering an adjacent coverage of that service area, and also provisioning a high capacity and user throughput at a lower cost service per bit. Since most commercial satellites in orbit operating at the Ku-band currently provide large coverages for video broadcast services, there is a market opportunity for satellites which provide broadband data services using spot beam technology which employ Ka-band frequencies. The new high capacity satellite systems are capable of transforming the economics and quality of services that satellite broadband can provide. All the efforts to obtain advancements are driven by growing worldwide demand for different service which the most one is the Internet, particularly in mobility environments and by the orbital spectrum availability suggested by the Ka and Ku frequency bands. Principally, HTSs are considered as conventional spacecraft evolution. Technically, when a satellite provides coverage of the entire region of the Earth visible from the satellite employing a single beam, the satellite antenna gain is limited by the bandwidth. In general, each user must be equipped within a large aperture antenna relatively to support a high data rate, impacting the cost and the practically deployment. In addition, one stream of information only can be supported with a given frequency range. Subject to this condition, the spot beam approach has been massively used for satellite communication systems and it started using a few beams to a large number to cover most places in the regions of the world. [7] [8] [28]

Typically, spot beams are areas of signal reception on the ground and transmission reception in the spacecraft in discrete as utilizing by supporting antenna structures. In spot beam environments, the satellite provides coverage of only a portion of the Earth, normally a subcontinent, by utilizing shaped narrow beams pointed to various geographical areas. The positive point of this approach is a higher satellite antenna including a reduction in the aperture angle of the antenna. Furthermore,

the multi-spot beam approach supports the frequencies reuse for a variety of beams resulting effectively boosting the total system capacity. It is well known that the power of the satellite is a scarce resource. In addition to this, the traffic requirements of each intended beam may differ, and the reason can be due to differences of the time zones. It is noted that when a few beams use the same frequency, inter-beam interferences are generated following the non-zero gain of the antenna side-lobes. Thus, in the existence of this interference between the beams, the assigned capacity to each beam is determined by the power assigned to all beams. Consequently, it is critical to optimize the power assignment to each beam to meet the traffic demands. Despite these implied limitations, high throughput satellites are designed to provision admissible performance and capacity of the system. Typically, with HTSs, the service area is covered by a plenty of high gain spot beams with frequency reuse to support broadband services using small terminals. According to the performed test and research, utilizing numerous spot beam satellite can provide about 10 times higher capacity than traditional satellites using the same input power and equal receive station antenna size in Western Europe. To increase the bandwidth of the user accessibility and system throughput, HTSs utilize efficiency achievable with space division multiplexing as implemented by use of spot beam. Hence, HTS gain spectrum efficiency and boosted performance over the use of spot beam antennas in associated with ultra-wideband satellite transponders. [7] [8]

Color Pattern

As described before, HTSs have many beams to make an expandable use of frequency reuse. Typically, the beams can be arranged to provide coverage of a service region. Generally, in the concept of the user beams, four-color reuse patterns are used, and each beam is associated with one of the four colors, according to the frequency band and polarization. Moreover, in multi-beam concept, numerous frequencies are employed to use and both frequency and polarization differentiations can be utilized across the adjacent beams. In addition, other frequency reuse schemes are possible to use based on the spectrum available amount serving in each area. Following the four-color pattern concept, the term of the color is used to negotiate non-overlapping frequency bands, similarly subjecting to non-interfering by using different polarizations and this is driven from mathematical concept of four-color pattern theory. [7] [8]

As discussed, the four-color pattern can be supported with two various frequency sub-bands through the full Ka- and Ku- bands and two orthogonal polarizations considered as right-hand and left-hand circular polarizations. Following that, adjacent spots are of various colors, varying in frequency and polarizations and in figure 2.17, the spot beam coverage is shown. Thus, they can support the transmission of different information with no mutual interferences and spot beams including same color use the same frequency and the same polarization, but they are isolated from one to another spatially. Due to spatial separation, spot beams with the same color can support the transfer of different information. In most cases, the four-color pattern theory is the best resolution among system capacity and performance. Furthermore, other frequency reuse schemes can also be utilized. In some HTS systems, optimization is performed on total capacity

at the expense of wide area coverage and the reason is using on-board antenna geometries. The new version of HTS systems are designed to increase the bandwidth economics doubly of previous versions and concurrently provide much larger coverage areas and this is different in satellites in terms of the bandwidth increment. It is important to know theoretically that the frequency reuse factor of a multi spot beam antenna is the number of spots which can support divided by the number of colors but due to overlapping of the beams and other technical constrains, the real frequency reuse factor is normally decreased in real value theoretically. The design requirement for HTS tends to include in one or two categories, as implied before, first one in optimization of geographical coverage area and the second is the optimization of the performance of the RF link. One can thus categorize the systems that have emerged of late, particularly those types which are based on the Ka-band HTS systems through into two classes: those who are basically optimized to gain high availability links and those who are optimized considered for large geographical coverage areas. In former cases, it is characterized by the antennas that have beam widths of fractional degrees, the latter eases link performance to utilize larger spot beams. [7] [8] [28]

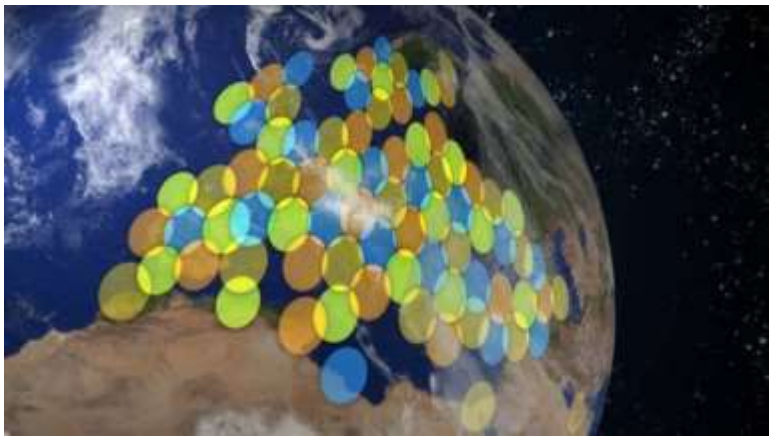


Figure 2.17: KA-SAT spot beam coverage [9]

To imply an HTS system, KA-SAT is a new generation of HTS system containing multiple spot beams providing a large capacity for a wide type of broadband service ranging from internet access in homes to satellite news gathering and domestic broadcasting applications. Briefly as a technical view, an HTS system includes the forward link and the return link. The forward link supports communications form a gateway to the users, while the return link is from the suers to the gateway. As an example, a broadcasting system can be specified as containing a similar architecture to that a forward link. [7] [8]

Spot Beam Approach

Generally, high throughput satellites classified as Ka-band small and large spot beam systems and Ku-band spot beam systems. Recently, some satellite operators tried to offer Ka-band capacity utilizing a small Ka-band payload on satellites that were primarily C or Ku-band based. The Ka-band beams typically are the beams with no frequency reuse and this approach had restricted the commercial demands. To obtain a high degree of frequency reuse, the broader geography of interest is no longer covered by a large single beam, but by a high number of overlapping which referred as high gain spot beams. Consequently, the cost per provided bit for the HTS design is remarkably lower than for a satellite optimized for wide broadcast coverage. Each spot beam reuses available frequencies and polarizations, following this an HTS is able to deliver up to approximately 10 times the capacity of former satellites and also the channel frequencies are reused multiple times in geographical non-overlapping spots, though the individual beams spectrum is limited through the available satellite bands, generally 500MHz in total. HTS payloads typically have 5 to 10 GHz of aggregate internal transponder bandwidth to aim supporting the throughput. These spot beams deliver high signal power and gain which referred as Effective isotropic radiated power (EIRP) and G/T, allowing the satellite to close links to small aperture Earth stations at a high data rates with suitable margin of the rain fade aiming to deliver acceptable overall link availability. Theoretically, there is no limitation to reuse the spectrum in multiple times and this can be done by beam isolation and achievable polarization discrimination purity.

HTS leverages frequency reuse through multiple narrowly concentrated spot beams as compared to former satellite technology which is based on wide coverage single beam. Each HTS spot beam covers an area of 1-2% the size of a common satellite beam and the size can be changeable as required. The reason is that the spot beams cover limited geographical areas. Typically, HTSs have gateway beams and transponders allocated to support connections with the gateway nodes on the Earth, especially where the traffic is handed over to the Internet or other networks. The critical element for the realization of a multiple spot beam coverage environment with overlapping spots is the satellite antenna. A principal HTS objective is to utilize a definite feed horns numbers in space fitted on a geometric matrix and illuminating a single reflector. Beam-forming techniques which are digital signal processing methods are used. [7] [8]

2.2.2. Integrating Satellite and 5G Mobile Technology

Terrestrial cellular mobile networks, which have evolved through several technology development generations, have not commonly contained a satellite communications component to any great scope. The cellular structure and emphasis on small, localized cells delivering voice and moderate data rate point-to-point communications, has not required satellite communications to deliver user-to-user connection. The one exceptional case is the utilization of the satellite for backhaul services for long distance and intercontinental connections and communications.

This lack of satellite links in terrestrial cellular service delivery is changing rapidly, however, as fourth generation (4G) mobile systems move into fifth generation (5G) technology. Satellite services, especially HTS systems, will play a leading role in 5G mobile networks. Before we discuss the anticipated major role of satellite technology in 5G cellular, a brief overview of the 5G mobile technology will provide a useful perspective on how satellite networks will fit into the 5G telecommunications infrastructure. Considering the previous new mobile generation standards have merged approximately every 10 years starting with first generation 2G, 3G and 4G, the first 5G deployments would be expected around 2020 year.

Subject to satellite 5G technologies, moving to 5G environment will see a merging of several technologies, which involve not only the traditional 2G/3G/4G terrestrial cellular services, but will notice an expansion of broadband high data transmission rate services and will comprise satellite and possibly high-altitude platforms as well as expanded terrestrial components. In the following, some of the technologies driving 5G implementation are described:

- Cognitive radio
- Machine to machine (M2M) communications
- Internet of Things (IoT)
- Screen resolution and video downloading incensement
- Software defined radio access technologies
- Cloud computing

The significant influence of these technologies is a fast-projected growth in traffic in the 2020 period. Three user trends that are leading the move towards fast traffic growth include increased video usage, "smart" device proliferation, and rapid acceleration of applications and downloading. The 5G environment expansion will include a convergence of service delivery via multiple networks and systems through the next years. The multiple networks will include fixed (FSS), mobile (MSS), and broadcast (BSS) satellites, operating in new and expanded frequency bands. The satellite delivery components will need very high capacity communication links operating on global distribution levels, extending the performance of HTS systems beyond current levels. New frequency allocations will require to be used to support the increased traffic capacity, and these frequency bands will be higher in the spectrum, where the bandwidth and unutilized spectrum is available to use. The requirement to move to higher frequency allocations for further generation

HTS has already been distinguished. To imply the wide broadband potential, certain frequency bands, which extend from 24.25 to 86 GHz, are proposed, however, the propagations problems, especially for satellite link distances, are large and should be evaluated.

HTS can be expected to deliver very high data transmission rate services in point-to-point, broadcast, multicast communications and delivery to small outdoor radio access points. Satellite-based networks will help to interconnect wireless access networks for in-home and in-building distribution, including in-building mobile users. Current typical HTS delivery of scheduled video and on-demand TV will expand as demand for downloading and IP services incensement.

The 5G ecosystem will contain a vast array of services and satellite delivery networks will play a major part in its implementation. The following figure 2.18 illustrates the integrated 5G network ecosystem in a global vision of the array of services and activities.

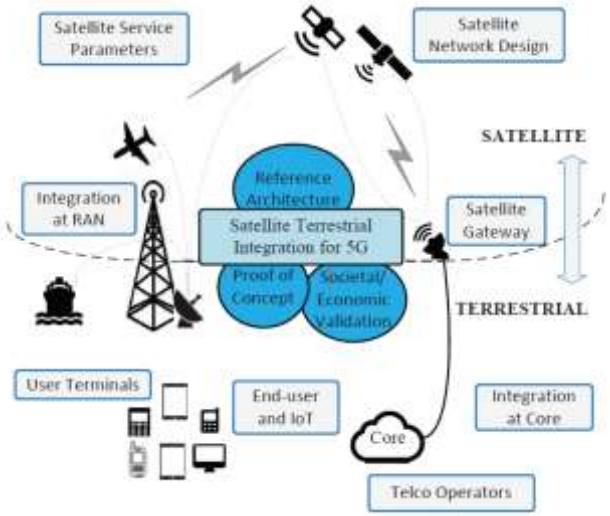


Figure 2.18: Integrated 5G network ecosystem [11]

Technically, 5G technology will require large blocks of contiguous spectrum, not available below 31 GHz. Satellite delivery will be essential to allow the development of the innovative planned broadband services, and Ka-band (and higher) HTS systems will be at the center of these networks. By the year 2025 one estimate future imaginations that there will be over 100 HTS systems in orbit delivering Terabits of global connectivity. Satellite HTS spectrum will be primarily at Ka-band, however, FSS allocations in Q/V bands are already under intense study and evaluation. [10] [12]

2.2.2.1. Satellite Role in 5G Technology

Considering the role of satellite in 5G, the leading areas where satellite can play this role includes the coverage and integration, resilience and overspill, content multicast and caching, Internet of things (IoT) over satellite network, software networking cognitive management across satellite and terrestrial interfaces, and spectrum. Regarding the first key area, satellites can deliver the wide coverage to complement and extend the aggregate terrestrial cells, which is fit with the ubiquitous coverage targeted by 5G networks. They will not be able to match the area spectral efficiency of the 5G terrestrial, but they are able to provide larger cells in a heterogeneous arrangement which can also be utilized for critical and emergency services and possibly to relieve the terrestrial cells of signaling and management functions in a software defined network configuration. Integrating satellites with the terrestrial system is perhaps the key area which enables many of the advantages. One of which is improving quality of experience by intelligently routing traffic among the delivery systems and caching high capacity video for onward transmission terrestrially. This can be empowered by the multicast and broadcast capabilities of satellite systems, while propagation latency is no longer an issue thanks to intelligent caching. Moreover, the traffic can be offloaded from the terrestrial system to save on valuable terrestrial spectrum, thus opening the possibility of improving resilience and security using the two networks.

The next leading role, which is resilience and overspill, satellites have a significant function to play in supporting the overall resilience by complementing other communications infrastructure. This role can support a resilient 5G network to mitigate the problems of overloading and the congestion. In content multicast and caching role, satellites have a leading function in content caching close the edge, fetching content closer to the user for acquiring zero perceived delay feature and providing 1000 times higher data rate and capacity in access to multimedia rich content such as global coverage with a few autonomous systems based on the satellite network, ultra-low content access latency, and offloading the cache content population from terrestrial networks. The role of IoT over satellite network provide the expectation of using trillions of sensors and devices will be connected through the 5G infrastructure, these sensors and devices will serve a wide range of applications in various fields. In cognitive management role, the mobile soft-core networks are new innovative platforms being developed by mobile industries to provide more flexibility for network deployment in environments with limited planning, build and operational support. Subject to the last role, which is the spectrum, a lack was emerged as one of the key drivers to the 5G network architecture. Technically, the demands on the network design could be lightened if more spectrums could be available. Furthermore, the frequency sharing on a dynamic principle between mobile and satellite systems can provide major incensements over the spectrum delivered both sectors accept the sharing basics. The techniques of data bases and cognitive radio can be designed and composed in future systems to allow frequency sharing. Resulting to this, situation to both sectors would be enhanced by employing an integrated approach.

Subject to using an integrated network approach, integration process between two various scopes of satellite communications and mobile wireless or terrestrial systems players has not always been

simple because of the stove pipe approach of each sector. Consequently, current satellite networks support basically 2G network backhaul for fixed sites with limited connectivity or emergency situations whereas 3G and LTE networks are currently following an extensive engineering attempt for standards adaption towards the specific satellite features. The recent emergence of a new 5G ecosystem with its convergence requirements delivers a unique opportunity to overcome some of the integration barriers, which existed in the past through development of a single environment from the initial development stages. Concurrently, it paves the way to enable two parts of the telecommunication industry to work together in order to define and specify a single 5G system with a holistic perspective. This guarantees that satellite communications can address the certain potential challenges in supporting the various envisaged requirements for 5G networks. [11]

2.2.3. KA-SAT Infrastructure Overview

The purpose of this section is to describe the KA-SAT infrastructure and the various relevant elements. This infrastructure presents the first new generation of high throughput satellite (HTS) system for broadband access services including variant service types. The total system capacity of the satellite can reach over 70 Gbit/s and has the capability of supporting up to a million users. The satellite has been configured with over 80 spot beams across Europe and North Africa, making it the most advanced multi-spot satellite designed in the world when deployed and four-color reuse pattern in different frequency bands and polarizations used to assign to each spot beam. By this, it includes the largest service-area by using frequency-reuse technique in which through this technique and everybody, regardless of distance, can access to homogenous broadband services. The system is equipped to use small terminals to deliver ADSL-like services to a million users utilizing adaptive coding and modulation algorithm where the coding and modulation are dynamically optimized for a given geographical area at the generic propagation conditions. [28] [30]

KA-SAT employs a highly developed payload technology with a spacecraft platform, and this minimizes development and qualification attempt and maintains general program schedules while maximizing the capacity for its intended service area. It has been designed to reduce the provisioning service cost in terms of each Mbit/s. The result of a complex optimization process that considers to system constraints such as operational issues relating to the communications system, performance, satellite location area, cost of system, satellite thermal issues, etc. [28]

KA-SAT includes the ground infrastructure consisting of the network segment of several main gateways in various locations in Europe connected to the Internet backbone, the network operation center (NOC), and major core nodes providing a full range of services to the end users. The transmission links in KA-SAT are bidirectional in standpoint of broadband traffic and two links can be defined as forward and return links. The forward link is transmitting data from the gateway to the users and is also referred to as outbound transmission. The return link is the transmission data from the users to the gateway and is also referred inbound transmission. Ideally, Ka-band is suited for the user link due to the enhanced antenna performance of the terminal. By using advanced adaptive coding and modulation technique, the propagation impairment at these frequencies are mitigated. The most significant parameter of the system is the system capacity which is separated mainly among the forward and the return link capacity exactly where the forward capacity has a prevailing importance for download rate provided to the users. Due to the existence of limitations in available spectrum and for increasing the capacity of the system, KA-SAT employs a multi-spot beam broadband coverage with a high frequency re-use order. [13]

Following the system components in KA-SAT system which its architecture is shown in figure 2.19, the main system is composed of two major segments including satellite access network, terrestrial transport network, and customer network and they are introduced as following:

- **Ground segment:** Typically, it is referred as satellite gateway Earth station. This segment consists of the radio frequency (RF) Earth station equipment, satellite modem termination system (SMTS), network operations center (NOC), data center, centralized core node (CN), gateways, and backbone network which are composed of routers, switches, firewall, etc. This segment is responsible for interconnecting the gateways, core, and backbone networks.
- **User segment:** This segment is also called end-user domain which is categorized into the user terminal and its relevant customer premise equipment (CPE) in which the terminal types include fixed user terminal (UT) and mobile terminal (MT).
- **Space segment:** This segment of a satellite system is included as basic operational segments like ground and user segments, and it is typically comprising the satellite constellation, the uplink and downlink satellite links working in Ka-band frequency, and other entities and elements which are described in section 2.1.3.

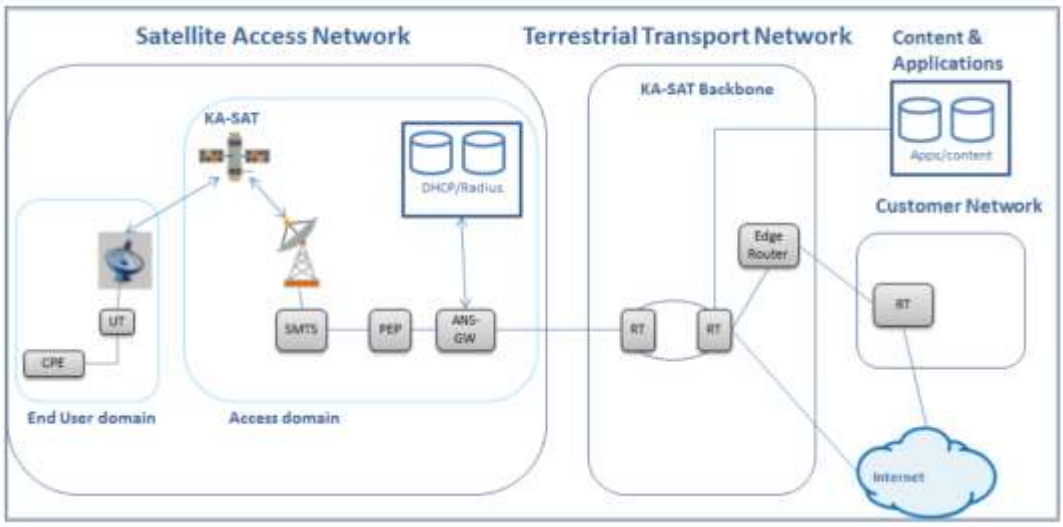


Figure 2.19: KA-SAT architecture overview as reference model [27]

According to KA-SAT system architecture, depending on the segment, there are various subsystems and entities which implied before. Each subsystem including its functions is discussed as the following paragraphs separately. [13]

Access Service Network Gateway (ASN-GW)

The access service network gateway (ASN-GW) is a centralized intelligent component considered as a major network component in the core node. Generally, it is responsible for managing and accounting all information flow between the users and provided Internet service and other applications such as authenticating and authorizing the user access. Moreover, it is referred as an entity which all the terminals required to be authenticated when they are going online and before start to performing traffic to the Internet as well. [13]

Network operations center (NOC)

This entity is generally placed remotely from the satellite gateways and is responsible for managing of satellite network and subscriber services through the network management and operations support. It is also supporting the various functionalities such as configuration management, performance monitoring, and network access security and audit. [13]

Traffic Shaper

This subsystem enables traffic throttling to provide the terminals including the subscribed service bandwidth. The operation is referred as packet shaping in which includes a set of controls on the traffic of a data network deigned to improve and optimize the performance or ensure the transmission, reduce and control the latency timing and make the bandwidth available over the queuing and packets delays which can meet the criteria as well. [13]

Performance Enhancement Proxy (PEP)

This subsystem which is operated as network agents is used to improve the employed protocol performance and mitigate the satellite latency as well. Moreover, the PEP servers are responsible for process the traffic of the users. [13]

Switches

In KA-SAT infrastructure, the switches are responsible for connecting physically all the network components to the backbone network and data center. [13]

Routers

The routers are the main network gateway components. Regarding the performing typical configuration, routers are used to connect to the backbone network. [13]

Provisioning

It is referred as a process in which the user is setup to operate on a specific graphical user interface-based platform to become online. [13]

Accounting

It is pertaining to the traffic volume which is generated by the user. Typically, each subscriber is assigned certain traffic based on the traffic volume threshold. [13]

Radius

Radius is considered as a server which is used for the authentication process of the all user terminals to be online on KA-SAT platform and the radius server does not work properly, the user is not able to go online. [13]

Firewall

This entity is referred as a network security device which allows monitoring incoming and outgoing traffic using a pre-defined securities regulation set. In general, it establishes a barrier among a trusted internal network and untrusted external network which can be the Internet. Firewalls classified into network or host-based firewalls. The network firewalls typically filter the traffic among several networks which run on network hardware and the next one run on host computers and control the traffic entry and exit of those systems. In KA-SAT platform, it runs security policies which allow the subscribers to be reachable from the Internet as well as mitigating security threats to the service platform. [13]

Dynamic Host Configuration Protocol (DHCP)

It is considered as an application protocol which allows the terminals over any network to receive automatically an IP network through every access request in which the IP configuration is required

to establish a connection and operate on a larger network. In the KA-SAT platform, DHCP is controlled by a DHCP server which dynamically allocates IP addresses to all terminals. [13]

Satellite Modem Termination System

To describe the satellite modem termination system (SMTS) which is comprising various subsystems, it is based on the advanced telecommunications computing architecture (ATCA) standard and is based on SurfBeam®2 technology, developed to make high availability systems which comprise redundant management, power, cooling, and board to board communications. Moreover, this system brings a new generation of affordable Ka-band wireless broadband services. The SMTS consists of a bank of satellite modulators and demodulators for transmissions to and from remote subscriber terminals. As a general view, it includes several blades placed in a chassis and contains forward channel and return channel as well. [13]

The SMTS performs all the real-time scheduling over the satellite traffic individually in which also provides air interface control for the network entity. Additionally, the SMTS controls the physical certain network interfaces and IP routing protocol support through direct connection of the satellite system within a standard routed TCP/IP protocol suit-based for terrestrial network. Particularly designed for today's emerging Ka-band satellite systems, the SMTS provides fast, reliable, high-quality bandwidth on demand intended for variant digital communication services.

This system is responsible for managing and controlling traffic between end terminals and the gateway routers and the servers. It performs all power and frequency management for both the forward and return links, and the management of satellite network bandwidth. A single SMTS system unit can process of each satellite bandwidth. One of the important features of SMTS is applying inter satellite handover for mobile user type aiming not to interrupt the service during moving from one beam coverage to another. In other words, it is implied that network orchestrated handover when online mobile terminals are entering another satellite's beam coverage from its current beam due to mobility operation. [13]

As described, one of important application of SMTS system is committed to provide IP interface between satellite network and Internet. It also provides medium access control (MAC) layer which is WiMAX based IEEE 802.16e standard and physical layer functions between gateway and user terminals. This system is be able to manage power, frequency, timing, and return link scheduling maps from user terminal point of view. The SMTS system is deploying several MAC domains for downstream and upstream transmissions for registered users and includes an association of one return channel group (RCG) and one forward link carrier (FLC) which referred as MAC processing subsystem (MPSS) as well. This enables to manage bandwidth allocations and the limits based on user's requirements. Moreover, it can support a great deal of subscribers even on given a single beam.

To consider the physical layer of this system, two forward and return links are available with specific attributes which are described in the SurfBeam®2 system section 2.2.3.1. To describe certain leading functions accomplished by various SMTS subsystems are signal modulating and demodulating, packet processing, and performing various corrections and power control algorithms aiming to measure adjust the user's transmit power level, forward and return link bandwidth scheduling, and common mode frequency tracking (CMFT) algorithm used to correct the satellite frequency drift due to Doppler effect and transponder translation through the gateways. To explain about CMFT algorithm, it consists of main parameters used in demodulators in which one parameter is for return link term, one is for forward link term, and the other parameters are used to help tracking operation in mixed populations environment. All these parameters belonging to one beam are shown in the figure 4.51 through the log analysis use case implementation section 5.1.4. Typically, the CMFT variations must be monitored and adjusted periodically in order to avoid upcoming issues. [13]

Customer premise equipment (CPE)

It refers to any terminal and associated equipment placed at a subscriber's premises and connected with a carrier telecommunication channel. CPE typically refers to a device such as telephones, routers, switches, any residential gateway, home networking adapters, and Internet access gateway. All these cases are provided Internet service by the service provider. The premises equipment consists of following components, outdoor and indoor unit, and an Intra-facility link (IFL) cable in which the outdoor unit includes an antenna, a ka-band transceiver referring as transmit and receive integrated assembly (TRIA) component. It is used on a satellite dish to process the signals to and from a ground-based system and a satellite. The indoor unit is referred as a modem and these two units are connected to each other by Intra-facility link (IFL) cable. [13]

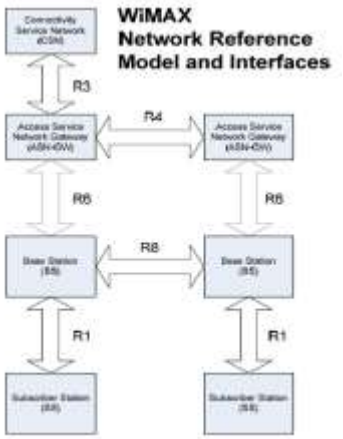


Figure 2.20: KA-SAT network topology [13]

In the next layer of SurfBeam®2 technology, the terminology of MAC domain is defined as one forward link and one return channel group relationship. In other words, the return channel group is associated with forward link. From user point of view, time slots are assigned to each specific user on any return link within an RCG in real-time status and this is done by time division multiple access (TDMA) technique. Conceptually, each user is registered on a specific return link. Following this, to support large-scale networks, the SurfBeam®2 system equipment resides in various locations, the user site which is called the customer premises, the gateway ground station, and the network operations center (NOC). Following that, the gateway ground station was discussed previously. Now, we proceed to describe the customer premises and network operations center, respectively. At the customer premises, each residential subscriber has a SurfBeam®2 user terminal, including two indoor and outdoor units in which the first unit is like a cable or DSL modem and the second unit like a dish for satellite television reception. This enables fast web browsing and video streaming, file transferring and other Internet applications at high downstream and upstream rates. A professional indoor unit and large outdoor unit support enterprise applications requiring higher speeds and availability attributes. Typically, the outdoor unit is composed of an antenna, Ka-band transceiver and feed horn is also referred as transmit-receive integrated assembly (TRIA) and indoor unit includes modem which is WiMAX-based and an Intra-facility link (IFL) cable.

The network operations center is generally placed remotely from the satellite gateways and is a key component of the SurfBeam®2 integrated management framework (IMF) applications reside. The basic application of the NOC is the management of satellite network and subscriber services through the network management (NMS), operation support (OSS), and business support (BSS) system. Typically, the NMS supports the functionalities of fault management (i.e., network status, alarms, event correlation, etc.), management of configuration, monitoring of performance, and network access security and audit. [13]

2.2.3.1 SurfBeam®2 System

In this section, we discussed about SurfBeam®2 satellite networking system which enables fast and cost-effective satellite broadband services. The design of the system delivers a wide range of mobile broadband communications, residential and enterprise services. The latest version of this technology named SurfBeam®2 includes the capabilities of high-capacity and high-performance in high-throughput satellites. Considering the full potential of Ka-band high-accuracy satellite, this technology can deliver more than ten times the speed and the capacity of current systems at a lower cost per subscriber. Achieving the capabilities of these satellites requires a complicated infrastructure to employ. With this, the operators can achieve the best user performance. By using SurfBeam®2 system, the satellites can deliver more than 250 Gbps of capacity to support around 5 million subscribers around the world. Delivering media-rich internet services such as real-time video, downloaded video and video social networking is an advantage with this technology. It also enables high-speed Internet, multimedia communication services to residential and business customers. The system design simplifies large network operations for service providers as an integrated management framework. The framework is comprised of three key sections of network management system (NMS), operations support system (OSS), and business support system (BSS).

The SurfBeam®2 system is satellite-based using broadband access network to provide high speed Internet connection to the users. It is also WiMAX-based on IEEE 802.16 standard. This standard adopted according to the target market in both fixed and mobile broadband services. The WiMAX network topology in SurfBeam®2 includes the following elements as network reference model and interfaces:

- Connectivity service network (CSN)
- Access service network gateway (ASN-GW)
- Base station (BS)
- Subscriber station (SS)

All these elements are associated with each other in the network topology. Explaining more about SurfBeam®2, the gateway architectures are comprised of two options, autonomous and aggregated gateways. In the first option, each gateway is stand-alone and self-contained and each one includes of its networking components. This approach is considered when the total gateways numbers are small. The second option is also called core node. In this architecture, various components such as acceleration, ASN-GW functions are centralized at core node locations for many gateways and each core node is ables to support and manage several gateways. The approach of this option adopted for many gateways. Generally, the Earth station consists of radio frequency equipment, satellite modem termination system, dish antenna and switching segment and the core node includes various sections such as Acceleration, ASN-GW, peering and traffic shaping parts.

In the physical layer of SurfBeam®2 system, two transmission links used for transferring radio wave signals in back and forth in a bidirectional path for each link. The typical link from the

gateway to the user is called forward link (FL) and reversely, the link from the user towards the gateway is called return link (RL). Typically, the return link concept is subject to return channel group (RCG) in which each one contains numerous return links.

In previous sections, spot beam concept and its specifications are discussed. To imply the spot beam, each user spot beam includes at least one forward link and one return channel group. In the following, the specifications of both transmission links are as below items: [13]

- **SurfBeam®2 forward link [13]**

Modulation/Coding:

- 16-APSK Rate 2/3, 3/4, 4/5, 5/6, 8/9
- 8-PSK Rate 3/5, 2/3, 3/4, 5/6
- QPSK Rate 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6
- Adaptive coding and modulation

Symbol Rate:

- 10 to 52 MSym/sec

- **SurfBeam®2 return link [13]**

Modulation/Coding:

- 8-PSK Rate 7/12, 2/3, 3/4
- QPSK Rate 3/8, 1/2, 5/8, 3/4
- BPSK Rate 1/2
- Automatic power control and rate adaptation:

Symbol Rate:

- 625, 1250, 2500, 5000, 10000 kSym/sec

2.2.3.2 Network Entry Procedure in SurfBeam®2

In this section, different phases are verified for entering the users in the network with focus on describing the user terminal interactions. As a general view, this network consists of various elements which include the MAC processing subsystem (MPSS) belonging to SMTS system, ASN-GW component, AAA and DHCP server, and acceleration server. All these sections are associated to each other and have their own interactions individually. The first thing that should be considered as a generalized structure is ranging process and the relevant physical layer adjustments accomplished between the SMTS system and user terminal. During this interaction, various processes will be performed respectively to associate at different levels.

In the ranging process, the user terminal attempts to synchronize its own physical layer parameters with the network entity. During signal transmission from satellite which is referred as forward link acquisition from satellite to user side, user terminal verifies three phases of broadcast messages to be prepared for ranging process. Firstly, user terminal examines to coordinate its time base with the intended network entity which is called setting time phase. SMTS system is responsible to carry out by sending and broadcasting specific messages. Secondly, user terminal examines the received information over configuration and return links location by receiving messages periodically. Through the last phase, user terminal verifies to locate initial ranging time slots. Accordingly, the initial ranging slots are contention access slots in which the user terminal attempts to transmit into them to create an initial contact with the SMTS system. Thereafter, once all information has been gathered, user terminal attempts to select randomly an initial ranging slot and then transmits a ranging request message to the destination point. During this, the initial transmission would be at an initial ranging power and this is configurable to make changes in power. To avoid occurrence of any potential collisions, Back-off protocols are used to resolve in initial ranging slot. After applying Back-off procedure, if no response received, the transmitted power is increasingly boosted, and the procedure will be repeated until the ranging response is received from SMTS system. The received ranging response message from SMTS system side provides necessary timing and power corrections to do synchronization the physical layer parameters of the user terminal with network entity. After finishing the initial contact process made by the SMTS system, the user terminal goes through a symbol rate discovery process. Following this, digital signal processing techniques used by this process to determine the maximum return link symbol rate in which the user terminal can operate appropriately. To assign an appropriate rate for the return link, the preferred operation for allocating return link symbol rate is typically accomplished by SMTS system and this is performed via transmitting a specialized message and after receiving the message, user terminal will declare its acknowledgement. All these described steps are ordinarily performed as interactions between the SMTS system and the user terminal to make an association to start the required conversation to transfer various messages as an initial process. [13]

After considering the required association between the user terminal and SMTS system completely as an initial step, the negotiation between SMTS system, ASN-GW and user

terminal is propounded as basic capabilities in the whole network system. These basic capabilities negotiation with SMTS and ASN-GW is performed by user terminal and this would be immediately after a successful ranging process and symbol rate discovery phase.

Typically, SMTS system uses a three-way handshake technique with the ASN-GW to trigger the initiation of the authentication process for the user terminal. In other words, user terminal authentication triggered when SMTS completes basic capabilities three-way handshake with ASN-GW entity. Thereafter authentication phase, it is the turn of registration phase of the user terminal in the network. Registration process is performed through which user terminal is allowed entry into the network. This phase includes negotiation of additional parameters plus those established in the basic capabilities exchange. [13]

2.2.4. Handover Technique

This section is aiming to discuss about handover technique concept plus its deployment performed by mobility manager entity through KA-SAT platform used for mobility service.

2.2.4.1. Overview

Since communications handovers concept are understood and used in the terrestrial mobile networks, this concept through non-geostationary satellite networks add additional complexity to satellite network designs, due to movements among the satellites and the satellites and ground Earth stations as well. Handover is responsible for maintaining the connection from source to destination points. Subject to this, satellite coverage moves across the satellite and links must be handed over from one satellite to the next one which is referred as inter-satellite handover term. For multi-beam satellites, handover technique is employed among variant spot beams which is referred as intra-satellite handover term, i.e. the mobile user moves from one beam to other beam within the satellite coverage area. Both described terms are shown in figure 2.21.

Whenever the next beam or satellite has no available link to employ the handed-over links, the links become lost and this results to force connection services termination and this event is classified as a handover failure term. Premature handover term is typically introduced as other forced termination reason in which creates in delayed handover results. Handover can be initiated based on the signal level strength and distance measurements position.

In general, the handover is carried out successfully when the satellite sends a message to the station informing it of which new frequency to use. In this handover case, the gateway is the intelligent entity. The time is required for launching and executing the handover technique must be very short. Besides this, the handovers should not degrade quality of service for the connections. Regarding the satellite constellation features, a terminal can be covered by at least two satellites. This provides the handover optimization possibility, with respect to the quality of service of each connection and serving with greater number of connections. [4]

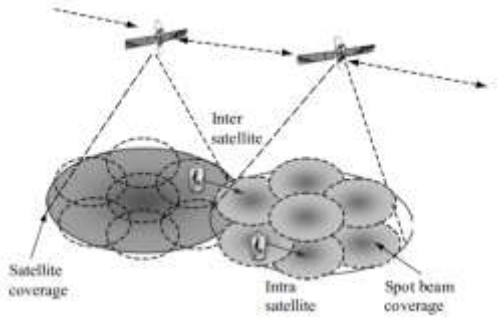


Figure 2.21: Inter- and intra-satellite beam handovers concepts [4]

2.2.4.2 Mobility Manager

Since in satellite communication, the handover technique is the process of transferring satellite control responsibility from one Earth station to another one with no service interruption and loss as well, this section aims to describe the mobility handover process concept through KA-SAT mobility service in which the handover algorithm is used to keep the service available and accessible for any mobile terminal type during moving from one satellite beam coverage to another one without interruption. As described before, the mobility services provided for any type of mobile platforms such as ground vehicles, boats, railway cars, and aircrafts, to participate in KA-SAT network.

The main element in deploying handover algorithm is the Mobility Manager (MM) subsystem in the ground segment of the KA-SAT network. This entity is located within each of the two major core nodes in the ground segment. In general, the Mobility Manager is responsible for managing and directing the handovers for all mobile terminals (MTs) between different beams. For instance, for one mobile terminal, this handover management is handled by the mobility manager entity from one satellite beam to another one.

Basically, the entities that are associated with each other to make and keep the service accessible and available during mobile terminal movement are including

Typically, there are certain basic mobility manager operations in the mobility handover process. Each mobility manager is responsible for making handover decisions for all mobile terminals operating in the satellite beam managed by the major core node at which it is located. A mobile terminal is communicating with the mobility manager entity periodically via sending a specific message which is called navigation data report (NDR). This message contains useful information such as terminal location, velocity, altitude, and other relevant data items. Each mobility manager possesses a database which is referred as a beam map contains all required data about the geographical coverage for each satellite beam on its operating network. Principally, the mobility

manager performs the handover based on its database when it receives the implied specific message from the desired mobile terminal to relocate form primary satellite beam to the target satellite beam. This procedure is fulfilled by querying the mobility manager entity from SMTS system supporting within its related gateway to do the handover algorithm. Summarily, the handover procedure is accomplished by exchanging end-to-end messages and various phases between serving and target SMTS systems, mobile terminal, mobility manager, and a certain set of interfaces such as radio resource manager which operate between these entities.

Considering this subject, the radio resource management (RRM) entity is introduced as an important subsystem in SMTS system to operate as an interface which includes a set of functionalities aiming to provide services based on the quality of service (QoS) negotiations for any application over the area covered by the system and optimize system capacity for choosing the best resource sharing among the users. Following this, the functionalities are including power control, handover algorithm, admission control, congestion and load control, and link adaption which all belongs to radio resource manager. [13] [14] [15] [16]

Consequently, the mobility manager forwards a handover directive query which identifies the target beam and other handover information to SMTS system supporting the serving beam in order to start the handover procedure. [13]

Part III.

Descriptive Study

3. Methodology

The goal of this chapter is to describe the methodology used in the thesis which includes monitoring tools introduction, use cases study, log analysis method and its role in satellite broadband., and dashboard design background as well.

3.1. Case Study: Splunk Enterprise Tool

The focus of this section will be on data logging and analysis procedure study in Splunk software as an expertise analysis tool. The significant subject that includes identifying various tasks in interaction data logging through visual analytics tools will be described.

To deliver an appropriate outline about the data and the analysis, Splunk and its data collection procedure is discussed. The main conclusion of this section is an explanation of the log analysis operations according to the queries that collected by Splunk and surveying the results. The data expose that log analysis is an operation which make sense with respect to the notable log analysis use cases such as troubleshooting and monitoring. [17]

3.1.1. Introduction

Splunk software is the single most powerful tool used for searching and exploring data. In other words, Splunk is a powerful platform for analyzing machine data, data which the machines emerge in massive volumes but that is seldom used effectively. Log analysis is one of the primary and earliest applications through data analysis in computer and information systems. Formerly, system developers began utilizing log analysis to understand and improve the performance of the system, availability, and usability. It used rapidly in various applications and domains dealing with data collection and analysis. Thus, users can analyze type of data sets by using Splunk in a wide range of fields or applications. Furthermore, Splunk users encounter different data analysis needs to use. As an example, in satellite broadband services and communications field, an operator might use Splunk tool to detect and identify the root cause of a system or component failure or any occurred anomaly to analyze and investigate the issue. According to this example, log analysis is a data type analysis where the data source is the data generated in machine.

Realizing how users analyze logs will help us to realize how users analyze data. Following that, Splunk data that we collected the logs provides massive records of how users analyzed logs in varied situations. [17]

3.1.2 Splunk Procedure

As described, Splunk monitoring tool is a powerful platform to analyze log messages comes from various systems or devices even in extreme volumes. The log messages are significant in the technology world and every day is getting increasingly important in identifying and detecting failures, anomalies and troubleshooting approaches as well. In the following, Splunk is described in detail as a Splunk case study and then different processes which are typically performed in this software, are discussed. The Splunk graphical user interface (GUI) example comprising various extracted fields and other information is shown in the figure 3.22. [17]

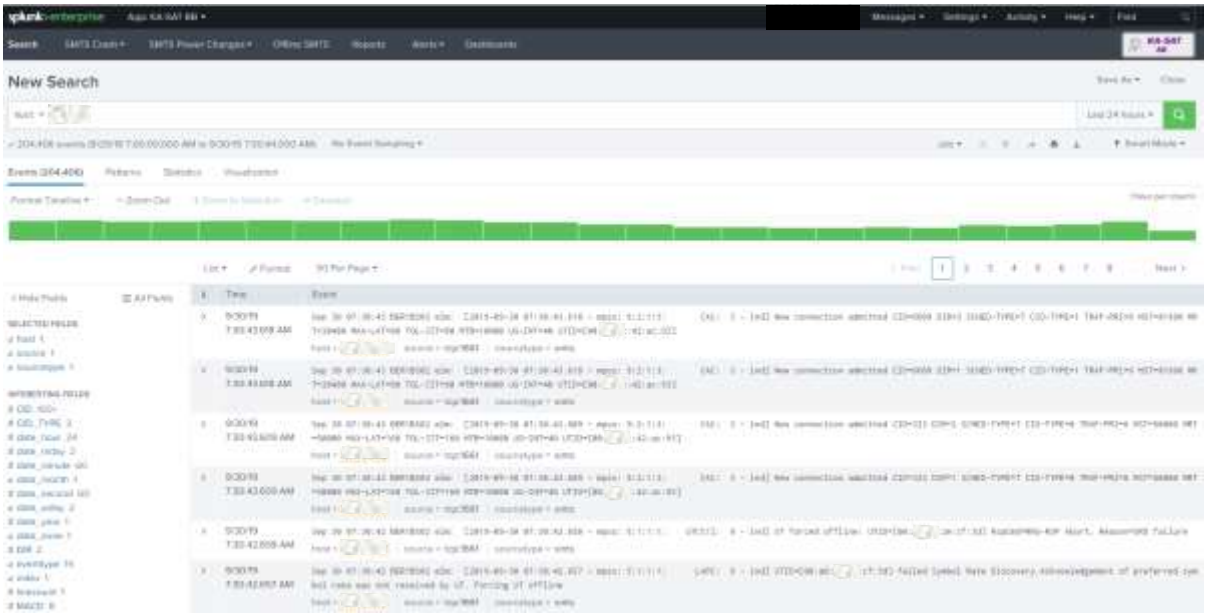


Figure 3.22: Splunk GUI example including variant extracted fields and event count statistics

In Splunk, there are important concepts to consider with focus attention to use this software in theoretical and practical standpoints. Initially, we consider these concepts in detail and then we explain the important core features of Splunk. Eventually, the major components of Splunk are described. The first element which is should be considered is an event term. An event is a set of values associated with a timestamp. It is referred as a single data entry and can have one or several lines. As an example, a typical event is shown as the following case:

Figure 3.23: Illustration of event log containing all extracted information about the event log

As we can notice in the figure 3.23, there are some significant parameters such as host, source, and source type. Generally, a host is the physical and virtual system name where an event originates. This can be used to search all data originating from a specific system through the infrastructure. Following that, the source is the file name, directory, and data stream. Sources are categorized into source types, which can be the desired formats defined by the user side. Since in this thesis, the focus of log analysis is on failures and anomalies occurrence, appropriate resolutions are provided aiming to troubleshoot and resolve the occurring recurrent issues.

By using extracted fields, user can search simply the name and value pairings which recognize one event from another. By using field, user can enter appropriate searches to recover the specific events that the user is interested. In processing the events at index-time and search-time, Splunk extracts the fields according to the definitions of a configuration file and user-defined patterns. Other important parameter which must be expressed is the set of tags. In general, a tag enables the user to seek for interested events which contain specific filed values. The user can assign one or multiple tags to any filed or value combination, including event type, hosts, sources, and sources types. By using tag, it is straight to group related field values entirely, or to track values of abstract filed by assigning them more descriptive names.

An important processing in which data can be read from a source on a host is index-time processing. This task is classified into a source type. During this process, timestamps are extracted, and data is parsed into individual events. Following that, line braking principles are exerted to fragment the events to display through the search results. In Splunk, each event is written to an index on disk, where the event can be retrieved subsequently by a search query. Through this process, when a search query is applied which is referring as search-time, indexed events can be retrieved from disk. In addition, the fields can be extracted from the raw text for the event.

In Indexing process, after adding data, Splunk tool initiates to parse the data into individual events, then applies line braking principles, and stores the events as an index. The user can create new indexes for various inputs and data is stored in the main index by default. The events are retrievable by one or more indexes through a search query. [17]

To explain the core features; search, reports, dashboards, and alerts are the most significant features in Splunk. The Search is the primary way users navigate data in Splunk expertise tool. As described, the user can write a search to retrieve the events from an index and this is done by using statistical commands to compute metrics and generate reports, searching for specific conditions through a rolling time window, identifying patterns in user's data, predict future trends, etc.

Accordingly, the user can transform the events using the Splunk search process language (SPL). Following this, all searches can be saved as reports and utilized to power dashboards. Mainly, the reports are saved searches and pivots. This enables for the user to run the reports, schedule the reports to run on a regular interval, or set a scheduled report to create alerts when the results meet specific conditions. The reports can be added to dashboards as panels.

The dashboards, they are composed of certain panels which contain modules such as search boxes, fields, and data visualizations. Dashboard panels are typically connected to the saved searches or pivots. They can display the results of completed searches, as well as data from real-time searches.

The next significant feature are the alerts. Generally, the alerts are triggered when search results meet peculiar conditions. The user can utilize the alerts on historical and real-time searches. Alerts can be configured to trigger typical actions. Furthermore, data model, pivot, app, and distributed search are additional features of Splunk aiming to do its responsibility appropriately. Subject to these implied features, pivot refers to the table, chart, or other visualization graphs. It enables the user maps characteristics defined through data model objects to data visualizations, without writing the searches manually. Moreover, the pivots can be saved as reports and utilized to power dashboards.

About the apps, they are configurations collections, knowledge objects, and customer designed views and dashboards. They can extend the Splunk environment to fit organizational requirements teams such as UNIX and Windows system administrators and other case, and Splunk can run several apps concurrently. Considering the other additional feature, distributed search provides an appropriate method to scale the user deployment user by performing separation the search management and presentation layer from the indexing process and search retrieval layer. Practically, the user can utilize distributed search to facilitate horizontal scaling for advanced performance, to control the access to indexed data, and to manage dispersed data.
Regarding the Splunk major components, forwarder, indexer, and search head are the main components of Splunk. The first component is a Splunk instance that forwards data to another Splunk instance is referred to as a forwarder. The indexer is the next component which is the Splunk instance which is responsible to index data. The indexer transforms the raw data into events and stores the events into an index. The indexer is also being able to search the indexed data in response to search queries. Typically, the search peers are indexers which carry out search queries from the search head.

The last component is a distributed search environment-based which is referred as search head component. Similarly, it is the Splunk instance that directs search requests to a set of search peers and merges the results back to the user. If the instance carries out only searching and not indexing, it is usually referred to as a dedicated search head.

The unique capability of Splunk platform is to index machine-generated data. By this feature, the searching operation is fulfilled quickly for analysis, reporting, and the alerts. The initial data is raw data type and Splunk indexes them by creating a time-based map of the words through data with no change or any modification in data. Before Splunk starts to search a data large volume, it must

index the data which are typical events. The following figure is depicted the unique features of the Splunk indexes. [17]

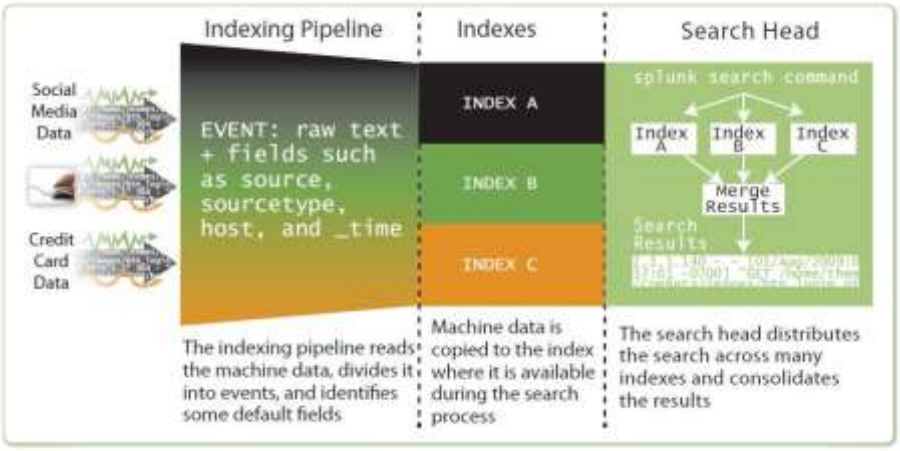


Figure 3.24: The unique features of Splunk indexes [17]

To summarize, Splunk can expose historical trends, correlate multiple data sources of information and help in different ways. In Splunk, the main phases are divided into three phases; identifying the data, which is referring as collecting data from various sources, transforming the data into the result and displaying them as data report, interactive chart, or graph to make easier finding the problems. It is feasible to make a summarization of the data in statistics or chunk of events as transactions, such as the entire log messages come from a component. Moreover, there is the possibility to create a workflow starting with data set, applying filter on non-relevant events, and finally analyzing the remainder data logs and generally, this implies a basic Splunk procedure. The figure 3.25, shows this process as three main phases. [17]

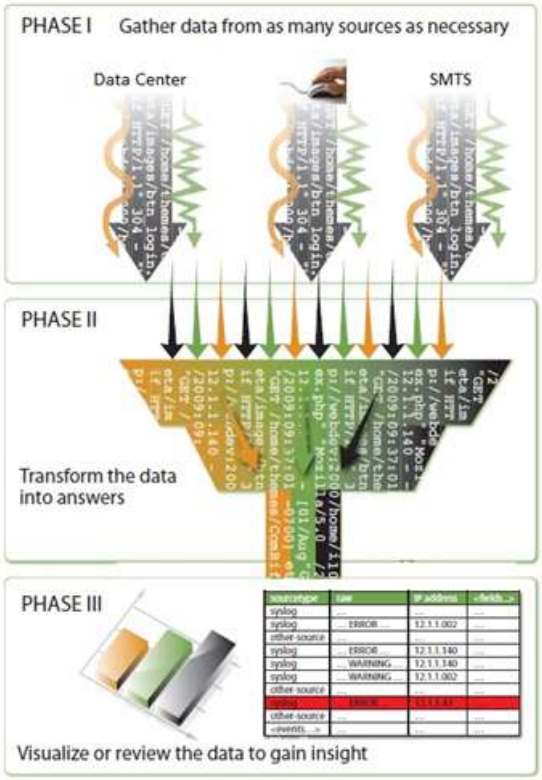


Figure 3.25: Splunk operation process [17]

Basically, there are three most common types of transformation through the log analysis which include filtering, aggregating, and augmenting. Subject to transformation use, the query stages typically are clustered containing these types of pointed transformations, and then verifying the transformations distribution across the clusters. The clustering operation is performed to recognize patterns of query stages use. The main goal is to attempt finding the desired patterns that are in accordance with to the user objectives and use cases, eventually to utilize such variables through the statistical models of user behavior, which can be used to make predictive interfaces. Clustering also provides an option to looking within a great number of examples to discover the patterns manually, but it is a time-consuming process.

Considering the transformation types, the filtering stages basically includes the search command use, which often all queries of Splunk start with, and allows users to choose events from a source and then filter them in various methods. This procedure is typically accomplished by clustering all different filter stages and discovered varied cluster types by using a certain number of features. The most common application of filtering is to utilize predicate logical conditions to refine a set

of events, which these predicates perform filtering operation for the other types, like those seek for desired matches of a given field or seek for an event with a specified string. [17] [18]

Another common filtering operation pulls data from a given source, index, or a host. These are like perform filtering that seek for a match in each field. To imply other filters types including those which do the deduplication in events, and perform filtering based on time range, index, and regular expression match. Eventually, certain filtering transformations comprise the utilization of macros, sub searches, and the arguments to constrain the filtering procedure. Resulting this, several points can be ascertained. Firstly, it is useful and helpful to treat log data concurrently structured and unstructured. To imply an example of structured case, it can be filed value-based filters and a string contains-based search. Secondly, certain commands in Splunk are extremely overloaded such as search option. By performing the redesign of the language procedure, the identification process of what exactly the users are doing will be easier. Finally, although the time range searches are not as common as might have be suspected give the time dimension importance in log data, the reason is that the time range is almost encoded in other parameters which are passed through the query. Consequently, the time is still one of the most significant filter dimensions for the log analysis standpoint.

The next transformation type is introduced as aggregating. By discovering a certain aggregate cluster types, it is possible to recognize how many features are used. One of the most common types of aggregate is to bucket the events temporally, aggregates each bucket, and then displays the aggregated value over period through a histogram figure. In general, visualizing the results of aggregations is a common task and viewing occasionally a table of the results is enough. The aggregations indicate the famous graphs that many users are familiar with them like lien and bar graphs. This is the same logically that users can visualize the filtering transformations results additionally. In augmenting transformation, adding, or transforming a field for each event is typically utilized. By clustering desired features, we can discover classes of augment. Subject to this transformation operation, users normally do transform their data by manipulating string, updating fields, and performing arithmetic. Moreover, calculating time information and applying multiple valued operations can be used to do transforming. [17] [19]

3.2. Case study: Nagios Monitoring Tool

The aim of this section is to discuss about Nagios monitoring tool that is used for monitoring the satellite gateway segment elements such as radio frequency chain components, satellite modem termination systems and networking areas throughout the KA-SAT platform. In the following, Nagios is expressed in terms of how it works and monitors the main infrastructure of KA-SAT environment. In the following, the applicability of Nagios in KA-SAT infrastructure will be discussed elaborately.

3.2.1. Overview

It is an open source computer software application that monitors compute systems and networks and the whole information technology (IT) infrastructure. By using Nagios, it is feasible to check and monitors system health checks and all infrastructure elements from physical and logical standpoints and entities. In other words, Nagios has the capability of monitor the whole infrastructure to ensure the systems, applications, and services are functioning properly. In case of occurring any issue or failure event, Nagios can alert related to the system problem by sending an email, a message, or other alerting methods. [21]

Nagios can be installed over a network, rather as virtual machine or running on physical hardware. There are four major elements in Nagios that should be monitored, and they are listed as following items:

- Centralized Nagios server
- The main networking concepts
- Alerting functions
- Visualizations functions

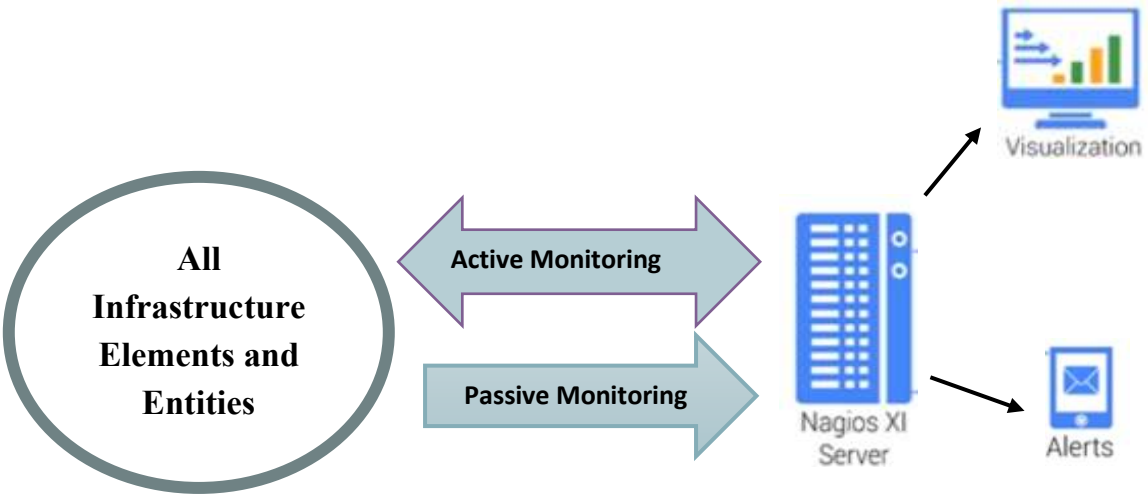


Figure 3.26: Nagios working process including active and passive monitoring

Technically, Nagios performs these monitoring tasks and activities by employing two methods: using an agent or a specified protocol. To describe about the first method, there is an agent enabled over a desired element and Nagios attempts to interact with this agent in order to obtain required information about the element. Thus, Nagios reaches out to this agent and then agent receives this information and then it responds back to Nagios. Now, Nagios checks this response and performs certain tasks such as storing the element information in which this information can be displayed as variant visualization graphs plus generating an alert. Therefore, that is a general view that how Nagios typically works. The main working Nagios process is shown in the figure 3.26. [21]

To explain the second method, Nagios has the capability of interacting with its network concept elements by using a native protocol which is simple network management network (SNMP). SNMP is a protocol that is designed for monitoring and managing various devices interconnected to a network. It allows the information can be retrieved from a device or system, setting options, and alerting for a device in order to notify that a failure occurs. Moreover, SNMP provides a standardized way to access information, called management information base (MIB). This explains which features exactly can be accessed, and what types of data are concerned with them. This implies the creation of features that all system or devices are forced to utilize to provide information on standard parameters. Thus, SNMP is introduced as a protocol to be implemented simply and is used to provide a way to access information on various machines and the figure 3.27 shows the main procedure of this protocol. SNMP includes several versions which an agent can communicate over. [21]

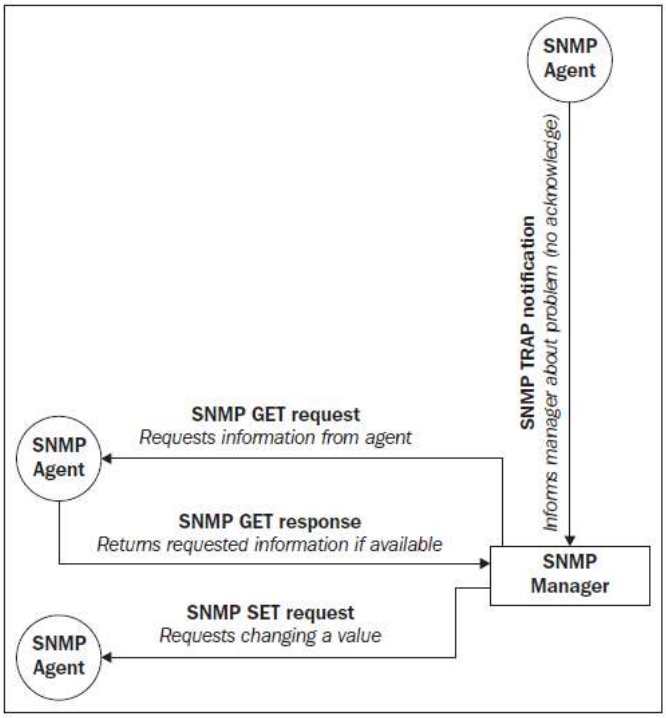


Figure 3.27: Illustration of various SNMP interactions procedures [20]

To explain the using procedure of this protocol, after enabling and configured the SNMP over the desired element, Nagios will reach out to the element and then element responds back, and this procedure is called active monitoring meaning that Nagios reaches out to the agent or to the network element by using a native protocol. There is another concept called passive monitoring in which an agent is used passively. The agent is placed and configured on the desired element and Nagios never reaches out to the element by the related agent. In this condition, the agent is just forwarding information about the element to Nagios regularly or when an event occurs and following that we can use this information for variant visualization reports, or we can use it for alerting purposes. [20] [21]

3.2.2. Nagios Applicability in KA-SAT

In KA-SAT, the monitoring activities for incoming alarms and alerts as status report are performed by Nagios monitoring tool and they are typically implemented over various elements of servers, switches, application, and services belonging to different areas. From technical standpoint, the events are generally triggered any time when a status change occurs through the platform. To monitor the implied entities for which the service is running, they are typically considered as host list in the platform. In Nagios, certain entities and elements such as satellite modem termination system, mobility manager, and all radio frequency (RF) chain components can be monitored in terms of checking service health, service status, and alarms and this is carried out by described simple network management protocol (SNMP) in order to accomplish as an agent for obtain required information from desired KA-SAT infrastructure elements and then forwarding to Nagios sever, and eventually provide this information as variant visualizations and alerts.

There are several important options in Nagios monitoring tool which used for minoring and they are including status, duration, attempt, last check, and status information. Nagios interface view including described options are shown in figure 3.28.
Considering the service status check, various status like warning, critical, unknown, unreachable, and Ok status containing their report summaries which solved, handled, or not, are triggered depending on the component status. According to figure 3.28, certain parts are explained and two uplink power control components belonging to two different gateway's RF chain are indicated as Ok status which means that they are working as normal and operative status.

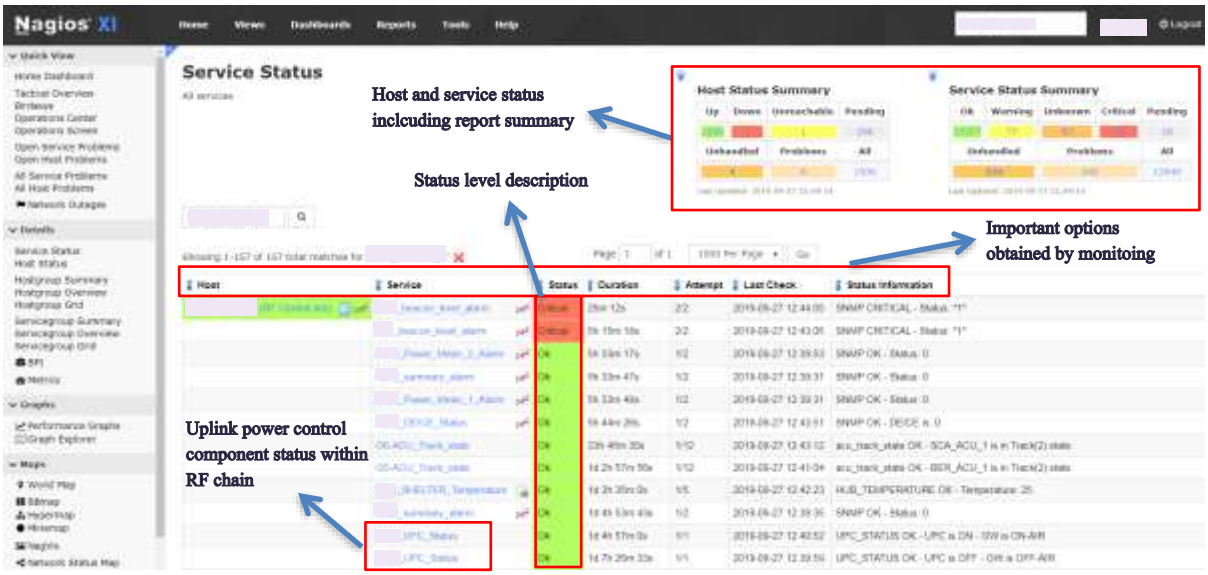


Figure 3.28: Nagios interface view including various information about the component and service status

Due to a specific reason, an incident or failure might occur in the KA-SAT platform areas and by using Nagios which is responsible for monitoring services elaborately in real-time, troubleshooting tasks can be carried out easily and effectively in order to find the element process breakdown rapidly by displaying alarms. In case of triggering any critical, warning, or unreachable events, the occurring event must be verified and resolved at once.

3.3. Use case

This section aims to discuss about use case concept and related techniques used for identifying a typical use case and then development process of a use case will be expressed.

3.3.1. Background to Use Case and Related Techniques

The use case terminology is a concept which is utilized generally for the system analysis approach and design procedure for providing a method of describing the user requirements. Principally, the use cases are designed to help in the management of the complexity through specifying the user requirements besides assisting in the user requirements development. The main goal of defining the use cases is to give the possibility to the users of a system to realize, verify, validate, and eventually test the requirements of a system which is once defined. Subject to this, various techniques and methods have been introduced to identify the use cases.

Regarding the analysis of a use case, there are several key elements to focus and explain. These important elements that must be considered as a priority to concentrate, includes the explanation of use case analysis, the procedure of performing use case analysis, identifying use cases methods, and writing proceeding a use case. The identification process of a use case has a significant role in our thesis. Basically, the use case analysis process is one of sub-element of analysis main element in a life cycle of system development. This implied cycle includes four major elements which are plan, analysis, design, and implementation. Typically, a use case analysis is the preliminary step to gather usage requirements for a task to be fulfilled. To imply one of the basic goals of this analysis it can be designing a system with respect to the user's perspective. [22]

To explain the definition of a use case, it is an activity which the system performs in response to a request by the user [23]. In another words, it indicates how a system interacts with its environment by presenting activities and tasks which are performed by the responses of the system and the users. Elaborately, the use cases are tools of explaining the user requirements and they are widely used in the analysis phase as well. There are two main techniques to develop use cases which are called the User goal technique and Event decomposition technique which are described in the following receptively:

- **User goal technique**

This technique is based on eight steps. Firstly, all users must be identified. Regarding their functional role and organizational level, they will be categorized. Hereafter, an interview must be accomplished to find the specific goals of the users. Creating use cases list according to a user type, seeking for repetitions, identifying the same use case where various users have, and finally reviewing of defined use aces are the left of steps of this technique. [24]

- **Event decomposition technique**

This technique is utilized for identifying the use cases according to the business events of the system which this enables the system handles and responds to that. This technique is the most comprehensive one that is used for identifying the use cases technically. As described, this technique starts to identify the whole business events which will cause the system to respond. This gives help to the analyst define each use case at the right level of detail corresponding to a task. In this technique, three event types are considered as external, temporal, and state events. An external event as is clear, it occurs outside the system typically triggered by an external agent. A temporal event occurs because of reaching a point level of the time and the state event occurs inside the system which triggers the requirement for processing.

To describe the steps of this technique, it includes seven steps. The steps of this technique comprises considering the external, temporal and state events in the system environment which require response from the system side, identifying and assigning a use case name to each event that the system needs, considering the state events which the system must respond especially in real-time which components triggers use cases.

Since event decomposition technique is the most known technique used for identifying use case, it starts by identifying all the business events the information system responds to, by considering each event leading to a use case. Regarding this technique and its steps to identify a use case in which used for defining a use case as a development process and eventually, six phases derived for building and running a use case. [24] [25]

3.3.2. Use Case Development Process

Regarding the use case definition concept, certain phases are used to define and run a use case based on the organization's requirements to achieve its objectives technically. In this research, this process is achieved by using event decomposition technique in order to identify and find a use case by performing a developed process in which is referred as use case definition. Subject to this description, a use case is conceptually considered as a development process for definition and as implied, it is including certain phases to be performed to build a use case. Considering this development process, the variant phases are listed and expressed as following respectively:

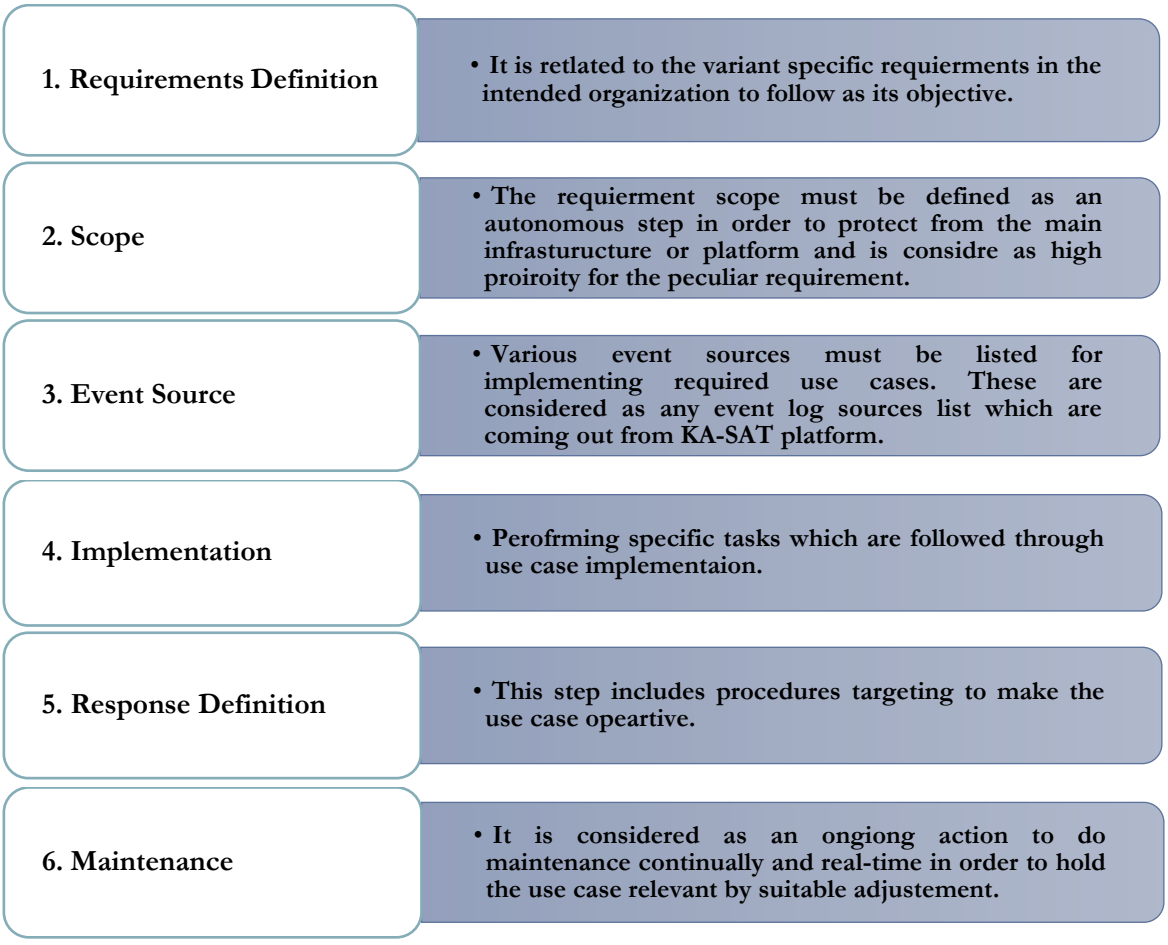


Figure 3.29: Use case development process steps

3.4. Log Analysis

The goal of this section is to introduce understanding and dealing with log data and its analysis. Log data comes in many forms and is generated by many types of systems. A long running problem is what one should do with all this log data and how to analyze it. This section presents techniques and tools that can help us analyze the log data. The structure of this section is based on describing background information on logging system and becoming familiar with various concepts of Syslog, SNMP, log data collection, filtering, and normalization, etc. Then we describe what a log message and have discussions include why the logs are significant. Continuously, we explain about log data sources emphasizing to describe the Syslog protocol, SNMP, etc. Moreover, various classifications of log data sources are presented. Next, we discuss about different analysis techniques and this is the principle requirement to be considered. In addition, we will discuss the process of responding to the results of log analysis. We will also explain how the log analysis can be reported in different ways and representing the way to define what the best reports are for log data. Following this, we describe the visualization methods of the log data. By visualizing we will declare what we are more interested in negotiating which is viewing log data in the context of directed graphs. Eventually, an advanced tool for log analysis and collection will be introduced and described in detail in do. This is considered as an open source and commercial toolset availability for the analysis and collection of the log data and by this the user can realize the right and best tool for analyzing logs based on the today's organizational needs.

3.4.1. Overview

The section of log analysis implies how to get a handle on system logs. In other words, it is about how to obtain useful information through the logs of all kinds. Logs, while often under-appreciated, are a very useful information source for a system source management, use and application management, and others. Analysis of log message or simply log analysis, deals with analyzing log data to derive useful meaning from it. Various disk storage components and products will log messages when a component failures or errors occur. Considering the logging data basics, at the heart of log data are log messages, or logs. A log message is what a computer system, device, component, etc. generates in response to some sort of stimuli. What precisely the stimuli are extremely depends on the source of the log messages. As an example, disk storage system will generate log messages when failures occur. Log data is the intrinsic meaning that a log message has. In other words, log data is the information pulled out of a log message to say why the log message is generated. The term log is used to imply a collection of log messages which will be utilized to paint a picture of some occurrence. In terms of troubleshooting, logs are valuable for this intention to help diagnosing issues and finding the root cause of the occurred failure in any system. Through this subject, Syslog standard designed for this purpose and we will discuss about the Syslog subsequently. Typically, log messages can be categorized into the following typical classifications:

- **Warning:** Messages of this type are concerned with situations where things may be missing or required for a system, but the absence of which will not impact system operation.
- **Error:** Log messages of error type are used to relay errors which happen at different levels in a system. For example, when a SMTS LMP disk is overloaded, it will generate errors logs and this may lead to make a failure. This overloaded LMP disk usage are divided into three types in terms of reaching to maximum capacity referred as a definite threshold, such as emergency and dangerous high disk usage, and exceeding of disk usage threshold.
- **Informational:** These messages are designed to allow the users and operators to know that something important has occurred. For instance, the SMTS will generate messages when the users suffer from disconnection issues through the network entry process on the KA-SAT platform.
- **Alarm:** This message type is used to indicate that something interesting occurred. As an example, the alarms which are generated in RF equipment due to being faulty, they can be seen in Nagios software which is an expertise monitoring tool utilized in radio frequency chain to monitor and other significant tasks.

3.4.2. Log data Transmission and Collection Procedure

Now, we will have a brief discussion of how log data is transmitted and collected. Typically, log data transmission and collection are a simple scenario conceptually. A device or a component implements a logging subsystem where it can generate a message every time it determines it needs to accomplish and this determination made depends on the device. In log message generation process through a device, there is an important requirement to configure the source system to log. There are three basic steps to enable logging task on most devices and systems which include enabling logging for intended device, configuring it to forward log message, and configuring it to send a loghost for next collection and analysis processes.

As an example, we may configure the device to generate a list of messages. On the other hand, we must have a place where the log message is sent and collected, and this place is typically referred as log-host. It is a computer system, normally a Unix system or Windows server, where log messages are collected in a centralized way and location. Subject to this, the advantages of using a central log collector type comprises a centralized place to store log messages from multiple locations, a place to store backup copies of the desired logs and a place where analysis can be performed on our log data. Now, time to describe how log messages can be transmitted in the first place. The most common method is via the Syslog standard protocol. This protocol is used for log messages interchange. It is typically found on Unix systems, but it is also used form Windows and other non-Unix based platforms. Conceptually, this is a principle client-server connection base approach. The client side is the actual device, component, or computer system

which generates and sends log messages. Then the server side typically can be found on a log collection server. Its principle task is to take receipt of Syslog-based messages and store them to local disk storage where they can be backed up and analyzed and stored the log-term utilization. Moreover, there are other options and mechanisms for log data transmission and collection. In general, they are sources and application commercially used which run on top of the Event log which will convert event log entries to Syslog, where they are sent to a Syslog server. To describe the Syslog priority, the message priority is to indicate the importance of a message. The set of priorities includes warning, error, critical, emergency, and indeterminate. [19]

Considering the following subject, to introduce the Simple Network Management Protocol (SNMP) which is a standard protocol used to manage networked devices. Principally, SNMP is a protocol for querying and configuring devices. SNMP traps and notifications are a specific type of SNMP message which is generated by a device or system when a specific event occurs. While the SNMP protocol entirely is not a logging system, its traps or notifications can be considered types of log messages. While many network devices are able to send event information via Syslog, some are not, particularly some older devices which referred as legacy devices (current legacy radio frequency equipment in Earth station), thus SNMP traps and notifications which referred as alarms are a method of getting event information from devices otherwise could not collect. And in some cases, the type of information sent via SNMP is different than that sent over Syslog. Regarding the SNMP protocol, there are two significant elements called managers and agents. SNMP managed devices are typically controlled by a network management station (NMS). The NMS polls devices periodically, querying for status information, forwards configuration changes, as necessary. The NMS also listens for traps or notifications. In this manner, the NMS functions similarly to a centralized log collector. The precise method of configuring SNMP traps varies with each other.

SNMP protocol is according to the two main concepts including traps and polling. To describe the trap, it is a form a log message which a device or system emits when something important has happened. Then it is sent to a management main station, which is like a loghost. The following management station is used to manage SNMP-based systems. To imply another concept, the polling is the place where the management station can use SNMP to make a query a component for pre-defined variables like interface statistics, bytes transferred in and out on an interface, etc. The main difference between the SNMP and Syslog is that SNMP must be structured regarding the data format.

Technically, databases are used for applications to store log messages. This means that instead of generating a Syslog message, an application can write its log messages to a database schema. Alternatively, in certain cases, the Syslog server can individually and directly write a relational database type. This is an advantageous approach, particularly in providing an organized method to store, analyze and report through log messages. [19]

Following the log message description as we discussed, a log message is something which generated by certain device or system to indicate which something happened. Considering this

subject, the common principle contents through a log message includes Timestamp, Source, and Data. These main items are always belonged to the message. The Timestamp indicates the time in which the log message was generated. Next one which is the source, implies the system or device which generated the log message. In KA-SAT platform, this is typically represented in hostname format through the Splunk software. The precise method a log message is represented depending on how the source of the log message has implemented its log data system. As described before, Syslog is the most popular format utilized by devices and various systems. The figure 3.30 represents the procedure of log data transmission, collection, and visualization.

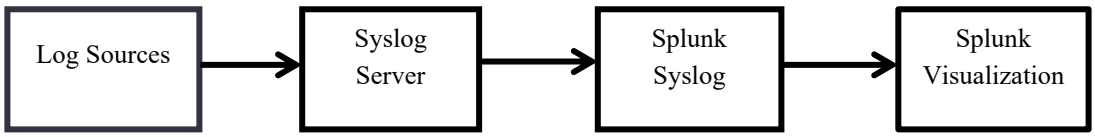


Figure 3.30: Diagram of log data transmission, collection, and visualization procedure

The following example provides a log messages in KA-SAT platform relating to the one SMTS system.

Jun 24 19:00:05 GWBS elm: [2019-06-24 19:06:73.983 - mpss: 6:1:1:5: CAC: 3 - ind] New connection admitted CID=528 DIR=1 SCHED-TYPE=7 CID-TYPE=0 TRAF-PRI=6 MST=50000 MRT=50000

This example shows a Syslog message generated from one SMTS system belonging to one base station including GWBS-ID name within KA-SAT Earth station and received on a loghost running a Syslog server. As it is clear, the timestamp includes the month, day, hour, and minute and including other information about the subsystem name of SMTS which is called MAC Processing Subsystem (MPSS) is shown. Considering this subject, one of the basic pieces of information which can be relayed in a log message is the priority level of the log message. From technical point of view, this is an interpretation of what the priority of the log message is, and this is often referred as severity. It must be noted that the Syslog protocol has an inherit priority scheme as well.

3.4.3. Filtering and Normalization in Log Message

Once a system or device is configured to generate log messages, filtering and normalizing of the messages are next steps to do. Filtering deals with including or excluding log messages based on the content in the log message. Originally, some sources support this attribute, or in some cases, we might employ an agent use in which intercepts effectively log messages and filters them according to the user defined rules. To decide exactly what to filter depends on the intended organization's requirements. For instance, it might be completely legitimate to drop SMTS reboot messages thorough maintenance. The next task to do is normalization. The normalization is the process of taking disparately formatted log messages and converting them to a typical format. The term of event is commonly used to indicate a normalized log message. As a matter of fact, when the log data is in a typical format it facilitates to manipulate the data, and this can be derived from it. It is noted that the normalization process is not using any source or standard protocol. To imply a normalization process, the following example indicates this normalization process:

Jul 16 03:00:08 GWBS elm: [2019-07-16 03:05:08.586 - mpss: 9:2:1:7: CAC: 3 - ind] New connection admitted CID=109 DIR=1 SCHED-TYPE=7 CID-TYPE=0 TRAF-PRI=6 MST=50000 MRT=50000 MAX-LAT=160 TOL-JIT=160 MTB=10000 UG-INT=40 U

There is useful information in this message. To do normalize for this case, we use a technique called parsing. Parsing includes scanning the log message from starting point to finishing point to pull out information that we are interested in and place them into normalized fields in the event. Regarding this example, the following items are typical fields utilized for normalization process. [19]

3.4.4. Collection tool for Log Analysis

The current market for log management and log analysis tools has advanced significantly over the years. Many toolset choices are built and designed into many of the current servers and network devices in use in environments today. We will deeply discuss and consider open source solutions and a commercial tool Splunk in next paragraphs to help us centralize, manage, and report on logs inside our environment. The tools range from basic flat file searching, centralized collection of logs, and all the way to more robust tools that incorporate compliance-specific reporting and real-time alerting. The tool that is right for us will depend on the number of or devices systems being monitored and our organization's compliance requirements. This section is not intended to be all encompassing but will review Splunk log management and log analysis tool widely available today

and provide details on the tool and features most applicable to daily log management in our organization. To introduce Splunk log analysis tool, it is a commercial offering tool which provides a wide range of features. Splunk will allow us to centralize our desired logs for forensics and correlation as well as generate real-time alerts based on the types of events that need further investigation or action. A key difference with Splunk is the wide variety of log sources it supports, real-time dashboards to review activity, customizable reporting and dashboards, and vendor-supported APIs to help integrate Splunk into our infrastructure. In next, Splunk enterprise software will be discussed in detail. [19]

3.4.5 Reporting and visualization tool

Reporting and visualizing are considered as the most significant attribute of a log management system and are regarded for technical support and operational activity purposes as well. Splunk software is contained large variety of capabilities and the analytics software particularly use for log analysis process in KA-SAT platform. [19]

3.5. Log Analysis Scope in Satellite Broadband

In satellite broadband, the systems and applications are evolving continuously in a high dynamic way and following that creating many disjoints among the systems and the operations technical support teams and other areas. This presents delays in service accomplishment and cycles of service assurance. Resulting this, most of the time the broadband service operation teams of these systems will spend long times to identify the root cause of occurred issues and anomalies raised by the users as a disconnection complaint. A vision through the system events will create a platform aiming to resolve these delays. Furthermore, this presents a general review of the entire performances of the infrastructure of intended organization and services suggested with these applications.

Considering this, the system logs as a fundamental and major input source will not typically give the required qualification for the analysis process when the data logs are unstructured form. When the log data are structured, the logs and syslog can provide the precise data. This indexed data requires to be transferred to an organized and effective search engine which is text-based which can be used based on the business requirement to monitor.

3.5.1. Adopting Log Analysis Approach in KA-SAT

Regarding our organization 's requirement, we are going to implement this approach to analyze the occurred incidents and events pertaining to KA-SAT platform. Accordingly, this approach is based on Splunk enterprise software aiming to analyze the event logs in various types. To briefly introduce some key capabilities of Splunk tool in log analysis approach, they are including as following items:

- Collecting of a great volume of event logs from various components and device
- Store the event logs for a definite period time
- Searching rapidly capability
- Presenting an explicit interpretation of event logs
- Correlation capabilities used between logs collected from various components and systems as log transaction
- Reporting capability

Following this, something is important to be highlighted through adopting this approach. Considering this approach, using a professional and technical logging process as a program is essential to utilize. Because, using this implied tool makes the implementation of the approach

easier. As described before, this tool is performing the process of collection the logs by using a specified protocol from various components and systems and then transform them to their specific format. To identify basic and main areas in terms of organizational requirements is important to note. This will assist to perform log analysis approach aiming to provide solutions properly through the infrastructure. As an example, if the requirement is monitoring data, then the starting point might be control requirements in which to notice what logs needed to be collected to fulfill them, and thereafter see how transaction and integration required to be done and eventually what required to be reported.

3.5.2. Log Analysis Use Cases

Regarding the benefits of the log analysis and its tool which it saves time required to detect and troubleshoot an issue or anomaly, it can improve the effectiveness and efficiency of operational processes and services in various areas. The use cases of the log analysis are as following:

- **Resource Management Use Case**
  The existence of the logs is beneficial for managing, maintaining, troubleshooting, and improving performance for any satellite platform systems. The most typical applications for log data in the KA-SAT infrastructure include monitoring cross-service through the system to detect specific log events and identifying patterns in log data, real-time monitoring activity for anomalies occurrence, analyzing the components health and the system, performance or configuration issues, and the root cause analysis.

- **Troubleshooting Use Case**
  Log data assists the technical operators rapidly exploration on any component related crashes and failures which comprise identifying poor performance areas, evaluating component health, and troubleshooting, and diagnosing and root cause identification of component installation and real-time error logs.

- **Performance Improvement**
  This concept is one step beyond the troubleshooting which is using useful information collected from the logs periodically aiming to predict and prevent incoming failures and crashes before they happen. The log analysis can improve the performance by detecting the incidents in the intended platform and infrastructure.

3.6. Background to Dashboard Design Process

A dashboard is a graphical user interface containing significant information that provides key performance indicators (KPIs) in real-time pertaining to a set of specific goals for KA-SAT system in order to report in variant ways technically. Moreover, it provides a comprehensive set aiming to view all activities across KA-SAT system for which log events are forwarded to a monitoring tool such as Splunk expertise tool. Dashboard allows to create variant visualizations of the results obtained from intended queries based on the event log data that display issues and as a result help to identify anomalies occurring in the platform. [26]

Using analytics dashboard facilitates the complex visualizations of entire analytics results and helps to communicate the insights with collected data on the dashboard as well. In other words, it allows to manage and monitor the contribution of various elements in KA-SAT platform. This aims to evaluate precisely how well KA-SAT service is performing well in terms of being operational. This would be feasible by capturing and reporting specific information points from each element within the KA-AST platform to emerge a performance view. To describe the advantages of dashboard, visual presentation of various performance scales and measures, capability to identify the root cause of the occurred anomaly or incident, generating reports with trends elaborately, and making more informed decisions according to the collected data. In order to have a well-qualified dashboard, the key elements of simplicity, communicating with ease, least level of distractions, supporting the organization with useful and meaningful data information.

Since log analysis resolves across two major activities referring as monitoring and troubleshooting use cases, by tracking key performance indicators in real-time dashboards, anomalies and incidents identification occurring in the platform would be feasible and easier. Whenever an abnormal behavior occurred through the platform, a powerful tool is required to dig profoundly into event log messages to find the root cause rapidly.

Subject to dashboard subject and its application, a development process including three main phases referring as a design flow and following subphases introduced for designing a dashboard. In the figure 3.31, the principle flow for designing a dashboard is shown.

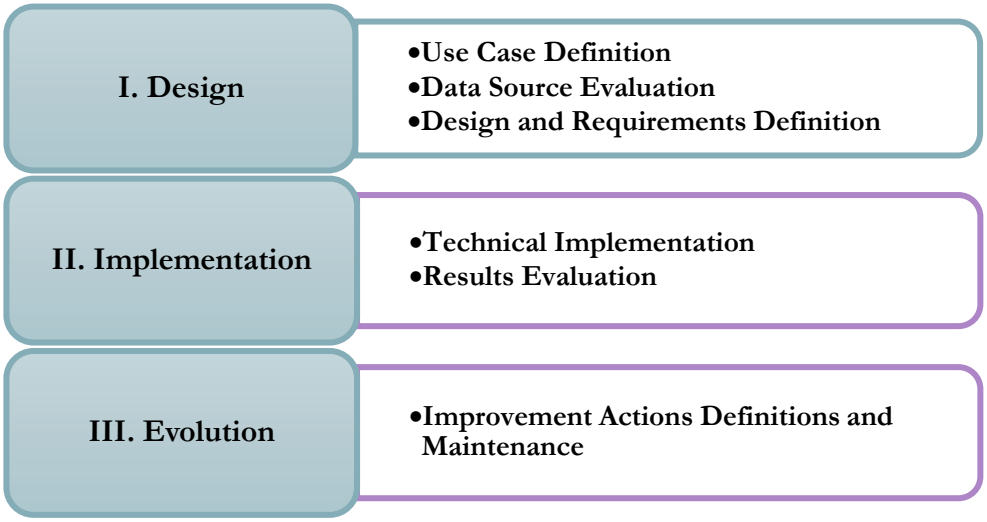


Figure 3.31: Dashboard design process

In this development process of designing a dashboard, all subphases are described as following items respectivly:

- **Use Case Definition**

It is related to a complete development process performed by certain steps to identify the main use case and satisfy organization's requirements. This phase is completely discussed in section 3.3.2.

- **Data Source Evaluation**

It defines the data collection procedure in terms of how, where, and what sources data must be collected from various sources. Hence, listing them for implementing the required use case.

- **Design and Requirements Definition**

To define requirement as a functional need for a peculiar design targeting to satisfy and is referred as high-level statements of objectives or needs of an organization. Requirement is used as an input into the design steps.

- **Technical Implementation**

Certain specific and technical tasks must be performed to resolve the issue and keep the infrastructure or system operational.

- **Results Evaluation**

It describes how to carry out analyzing data logs which is referring as performing root cause analysis, implementation process examination, and exploring and interpreting from results in order to improve effectiveness.

- **Improvement Actions Definitions**

It aims to simplify the root cause detection of anomaly from detecting to troubleshooting stage of activities and actions more effectively.

Part IV.

Analysis and Dashboard Design

4. Log Analysis for Event Detection Using Splunk

This section aims to provide information elaborately about real-time log analysis using Splunk enterprise software as a tool in KA-SAT infrastructure in both fixed and mobility. The main goal of this analysis is to perform monitoring data on the whole equipment and service impacts in the infrastructure to detect and any anomaly or failures and identify the root causes which this would be considered as a key element in this thesis to detect a crash over a component of a system in the platform. Following this, the major focus would be on generated log data from various systems and components through the KA-SAT platform. Hence, how this log data can be used and how they can be described. This will be done by using Splunk tool. As described before, Splunk is responsible for collecting and indexing the machine data, searching, and investigating for insights. It is possible easily to monitor and identify any issue which can be useful in maintenance and troubleshooting operations. With Splunk, the trends, patterns, and behaviors form data are possible to find. Eventually, analyzing and reporting extracted from data are the most leading features of this tool.

To explore the applicability of Splunk, the following example is the log data view in Splunk obtained from KA-SAT platform. At a glance, it sounds a complex view of log data due to existence of many events with different patterns and information. Based on the search item which is a user terminal (UT) search query, all generated data logs relating to the whole users extracted from all SMTS systems as source type concept belonging to the entire gateways in the KA-SAT platform. For instance, the information about the symbol discovery process failed in the user terminal connectivity procedure and other failures and information can be seen obviously. As it is clear, the certain significant sections are highlighted and explained as below Splunk interface in below briefly.

4.1. Fixed and Mobile Services

Regarding the log analysis for event detection using Splunk subject, Splunk utilization through fixed and mobility services are indicated and explained in the figure 4.32. According to this analysis which is related to entirely supported fixed-user terminals and mobile terminals by KA-SAT platform, all the required information and statistics in different fields are analyzed and indicated over a slot time.

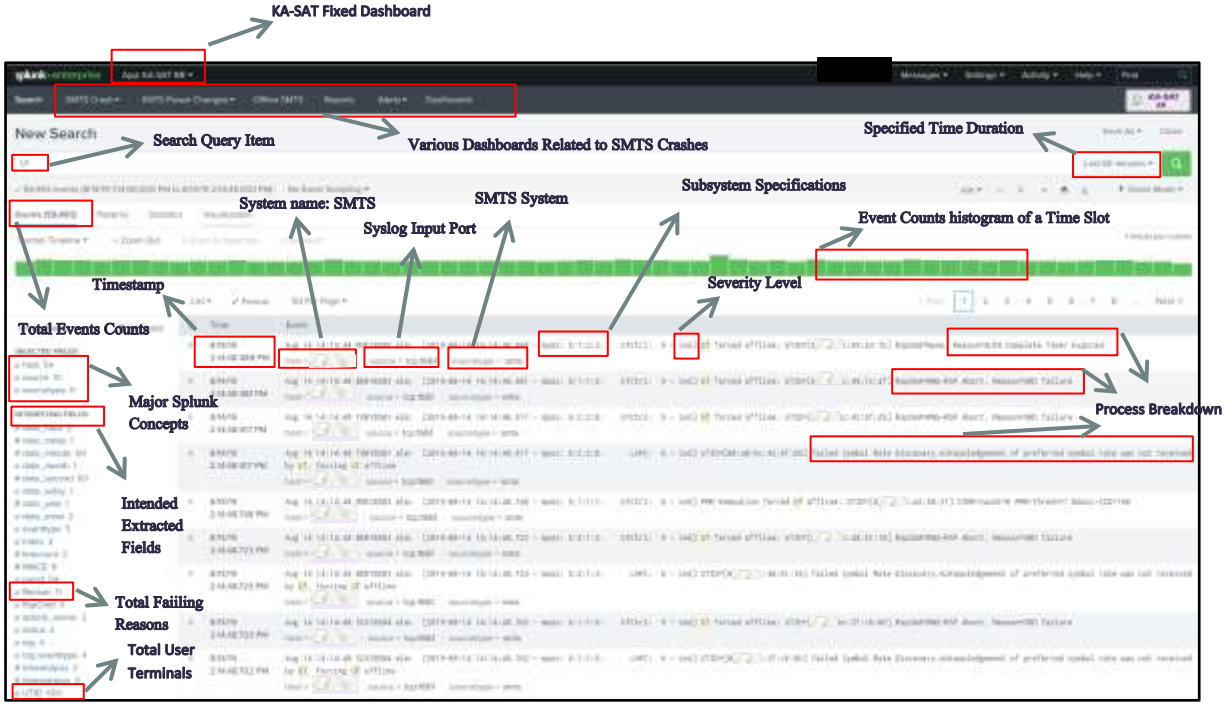


Figure 4.32: Splunk interface incluidng all required information about fixed-user terminals

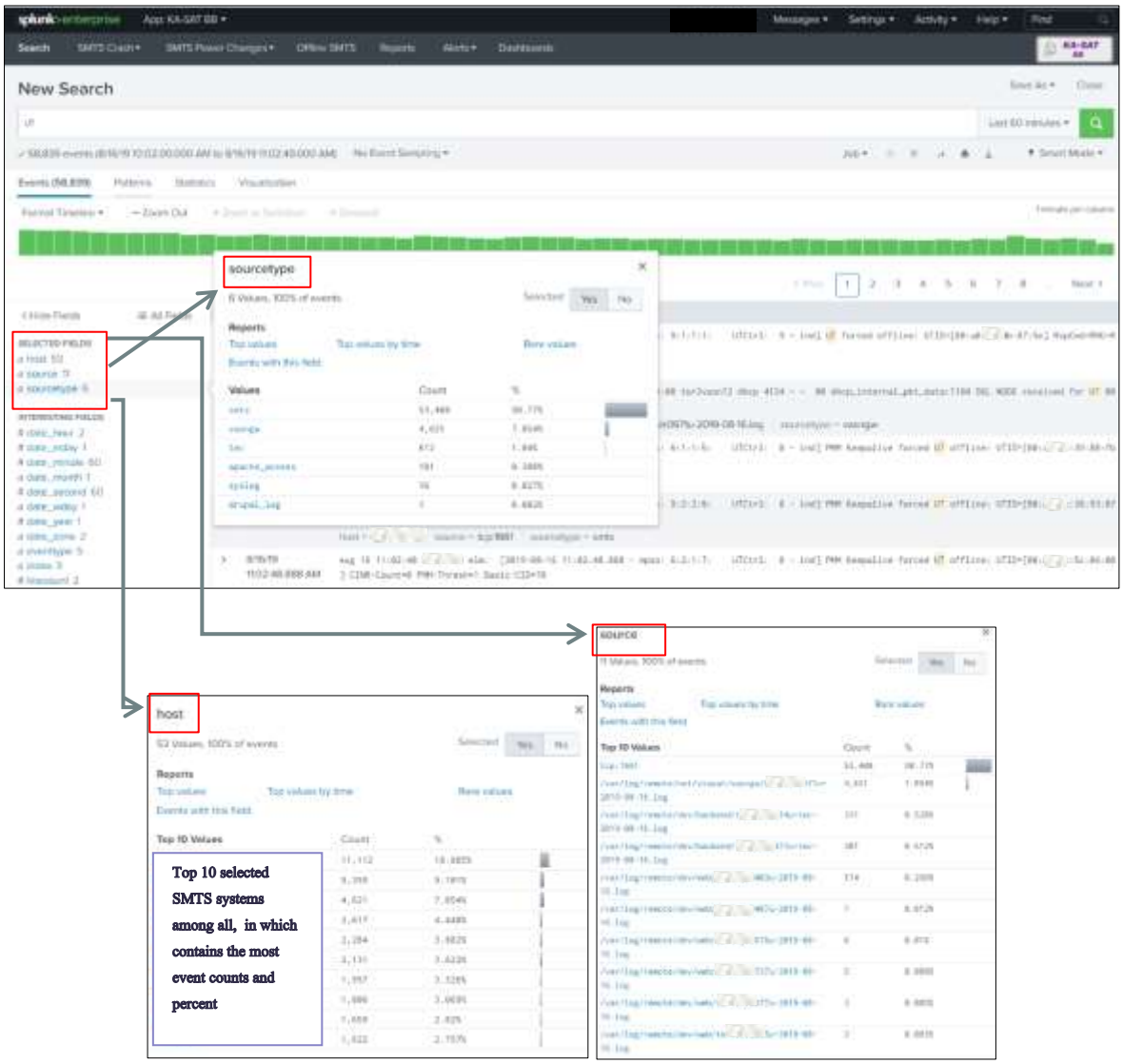


Figure 4.33: Splunk interface including description of selected major fields in details

In above Splunk KA-SAT fixed interface through the selected fields on the left side, the important items are described as following:

- **Host**: It includes all the SMTS Systems as physical devices belonged to their gateways in KA-SAT platfrom.
- **Source**: It is a list of event log files and Syslog Input specific port.
- **Source Type**: Sources are typically classified into source types at which the event logs can come from various sources such as a SMTS system, Syslog, or any independent entity.

Figure 4.34: Splunk interface including all required information about mobile-user terminals

In this Splunk KA-SAT mobility interface, the most highlited items as rectangular shape are similar to the described previous items in KA-SAT fixed interface and the remainder significant items are desribed in the figure 4.34 from technical point of view. In addition, the major Splunk concepts related to the KA-SAT mobility are mentioned as following selected fileds:

- **Host**: It is the employed mobility manager system as a physical device belonged to its relevant core node in KA-SAT platform.
- **Source**: It includes only a list of event log files.
- **Source Type**: This item comprises the entire type of sources pertainaing to the KA-SAT mobility platform such as mobility manager, Syslog, and etc.

4.2. KA-SAT Splunk Process

Considering the data source concept in which the data is originating and it is sending to the Splunk server, Syslog data source is introduced that within this server, all data logs are collecting by SNMP protocol from certain platforms in KA-SAT infrastructure such as SMTS systems, mobility manager, data center equipment (switches, routers, firewalls, etc.), and other sources, and then forwarding to Splunk server. This process is aiming to be accomplished for monitoring data, analyzing, and troubleshooting. Consequently, by using all these logs, the objectives of the mentioned process can be obtained and make sense the logs as well.
To describe the use of data logs efficiently and effectively, depicted three main operations and phases used by Splunk are explained as following items:

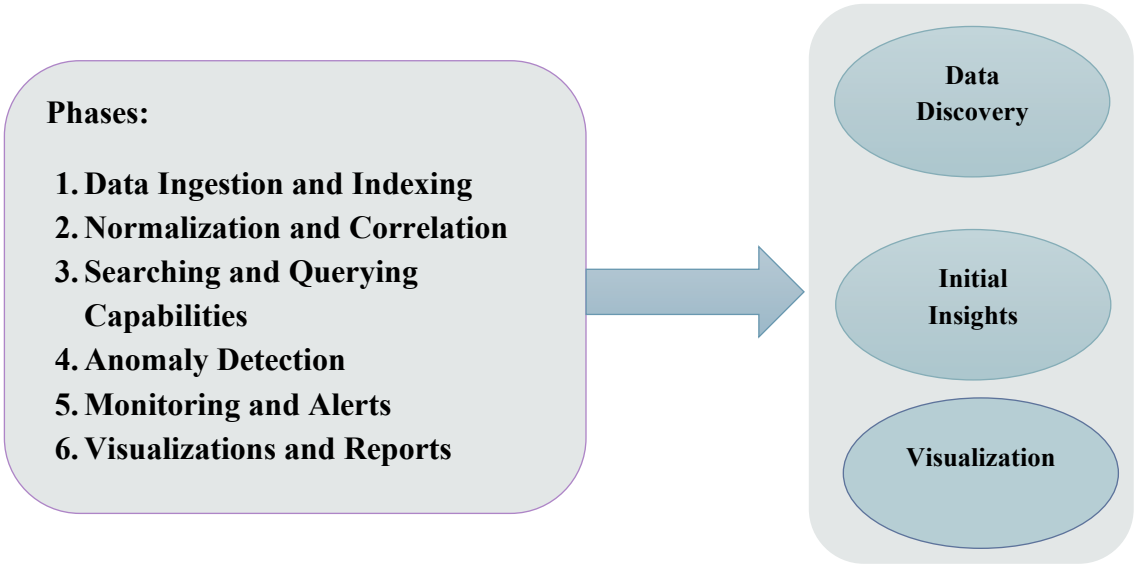


Figure 4.35: Splunk operation phases

Regarding the introduced phases in figure 4.35, various tasks and activities are performed as major operations in Splunk, and each is phase is explained as following:

- **Data Discovery:** In data discovery phase, which is referred as data identification phase, data is gathered and acquired as many sources such as SMTS systems and data center as necessary to explore and understand the data.

- **Initial insights:** In initial insights phase which is referred as transformation data phase, the data is transformed into answers or results that can solve the intended problem.
- **Visualizations:** This phase is responsible for visualizing the information via various visualization figures such as chart, report, and graph and this makes easier to find the problems for operators.

To explain the entire phases applied by Splunk regarding the KA-SAT platform, an integration of phases is completely discussed as following items, respectively.

4.2.1. Data Ingestion and Indexing

This phase aims to inquire various tasks in ingestion and indexing phase. These tasks include collecting a huge volume of data, performing automatic aggregation, normalizing through timestamps, and providing structure capability to unstructured data.
Considering the described tasks, Splunk can collect a great volume of data through forwarders which they are instances of Splunk that collect the data and send it to Spunk's deployment through the centralized location where the data is supposed to be analyzed any data volume and depending on our requirements, it is possible to scale. After collecting the data, is starts to aggregate the data by extracting the timestamp which is available in log files. This operation is referred as data normalization process. It takes the time stamps out of the data and once everything is up from latest event to the last one. In the figure 4.36, all data aggregated from entire SMTS systems belonging to one intended gateway has been collected for a quarter of an hour as events and it is around12,500 events. Moreover, Splunk can aggregate all the data and provide a comprehensive visualization report and thanks to this capability, we can notice the occurrence of high event numbers as peak and least values regarding the time axis. As we can see in the figure 4.36, the events are occurred in 15 minutes period in various amounts.

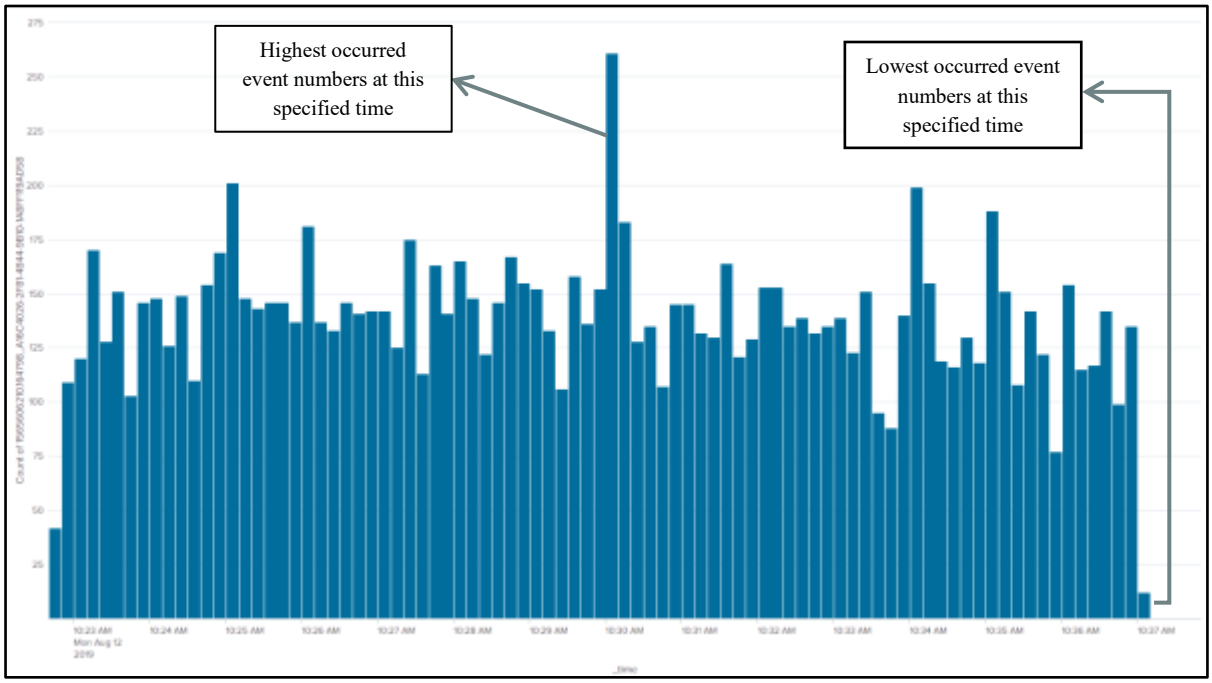


Figure 4.36: Aggregated events over time on SMTS systems supported by one gateway

As a result, this capability assists to provide a lot of information as all automated which is a great feature. To review the procedure, Splunk firstly ingest the data and then starting to index the data by performing normalization process it to timestamps. To imply a great attribute of Splunk, it has a very high-throughput capability and with this, it can ingest a huge amount of data in real-time. It is noted that there is no required to filter the data. Splunk has no format restrictions and this enables Splunk can read the most data formats and moreover, it does not require doing pre-processing or picking and choose and then forward a specific amount or type of data.
Splunk has the capability of giving structure to unstructured data. It means that we have a timestamp and large-scale information such as what event has occurred. This capability is fulfilled by normalizing into timestamps and it is possible to customize the desired indexes and by this, it will acquire a structure as the data is coming in.

4.2.2. Normalization and Correlation

To explain normalization process elaborately, if a great volume of data is collected from various servers, certainly this data collection would be in different formats. By performing normalization operation, that is possible to start comparing across different organizations of different types of data. Resulting to this, it is required to deploy a method to normalize the entire collected data and this is the key element and tough challenge in log analysis approach. Thanks to Splunk expertise

tool, this normalization process can be done automatically. To make an example to figure out how data can be normalized, three different logs written as following items:

Log A:

8/12/19 10:57:08.814 AM	Aug 12 10:34:08 GWBS-ID elm: [2019-08-12 10:57:87.814 - mpss: 5:2:1:3: CAC: 3 - ind] New connection admitted CID=6426 DIR=2 SCHED-TYPE=7 CID-TYPE=1 TRAF-PRI=6 MST=81960 MRT=20480 MAX-LAT=80 TOL-JIT=80 MTB=10000 UG-INT=40 UTID=[01:14:55:06:08:10]
	host = GWBS-01 source = GWBS-ID sourcetype = smts

Log B:

8/12/19 10:56:56.347 AM	Aug 12 10:56:56 GWBS-ID elm: [2019-08-12 10:92:56.347 - mpss: 5:2:1:3: UTCtrl: 9 - ind] UT forced offline: UTID=[01:14:66:32:88:10] RspCmd=RNG-RSP Abort, Reason=SRD failure
	host = GWBS-03 source = GWBS-ID sourcetype = smts

Log C:

8/12/19 10:56:56.347 AM	Aug 12 10:65:56 GWBS-ID elm: [2019-08-12 10:56:44.347 - mpss: 5:2:1:3: LAPC: 6 - ind] UTID = [01:46:33:06:08:09] failed Symbol Rate Discovery. Acknowledgement of preferred symbol rate was not received by UT. Forcing UT offline
	host = GWBS-05 source = GWBS-ID sourcetype = smts

As it is clear to notice, all three different logs contain a lot of information. All these logs are connected to each other somehow regarding the assigned user terminal identification number which is common between each other. By correlating them, we can figure out what is happening. To correlate data logs through normalization process across different formats, Splunk uses regular expressions to pull out data or a primary key from various types of logs it is a very highly depending on the regular expression. Considering this, the complexity of data increases, and the varieties of sources formats increase as well and this results to become highly difficult to normalize and by using an automated tool like Splunk, this would be feasible to do. It enables to process a great volume of data which come in from different source and we are getting insights in real-time. As a result, correlation enables us to get deeper insights through the data logs.

4.2.3. Searching and Querying Capabilities

In this phase, once everything is set up and structure data provisioned in Splunk, then we can search and query easily. Splunk uses search processing language (SPL) and it enables to query data logs, build the data models, create the visualizations, and finally acquire intended insights. This is referred as ongoing process because as the data coming in as the data is exchanging to make sure to keep adapting these queries as the data is coming in real-time. When we gain more insights, then we can make sure that we address the user's problem or not and how we can make this better as well. Resulting to this, as more insight is acquired, the queries must be updated.

4.2.4. Anomaly Detection and Correlations

One of the key features of the Splunk tool is the anomaly detection which this is considered as an important concept in this thesis research. It is a pattern which is based on machine learning concept employed in Splunk in which assists to look for trends and patterns within the intended data logs. According to the figure 4.37, by looking at patterns section, we can find some important failures occurred, meaning that some processes being broken down not to do as their normal status. Regarding the search activity, 6 patterns were found based on a sample of 2,768 events within 15 minutes time interval. Thus, by looking through 2,768 events, we can find the trends and patterns in which 39.38% percent of the whole data logs is pertaining to a specific user terminal which is taken offline due to aborting of ranging process activity within a SMTS system's component of the relevant gateway and this typically results a failure which is referred as not enabling to perform symbol rate discovery operation applied between the SMTS system and the user terminal in order to interact with each other at a nominal level. Here, the entire SMTS systems are considered as a host concept in Splunk search section and UT offline item has been filtered pointing to the disconnection reasons. All the key elements are pointed out in rectangular shapes in our anomaly detection search and query activity depicted in the figure 4.37.

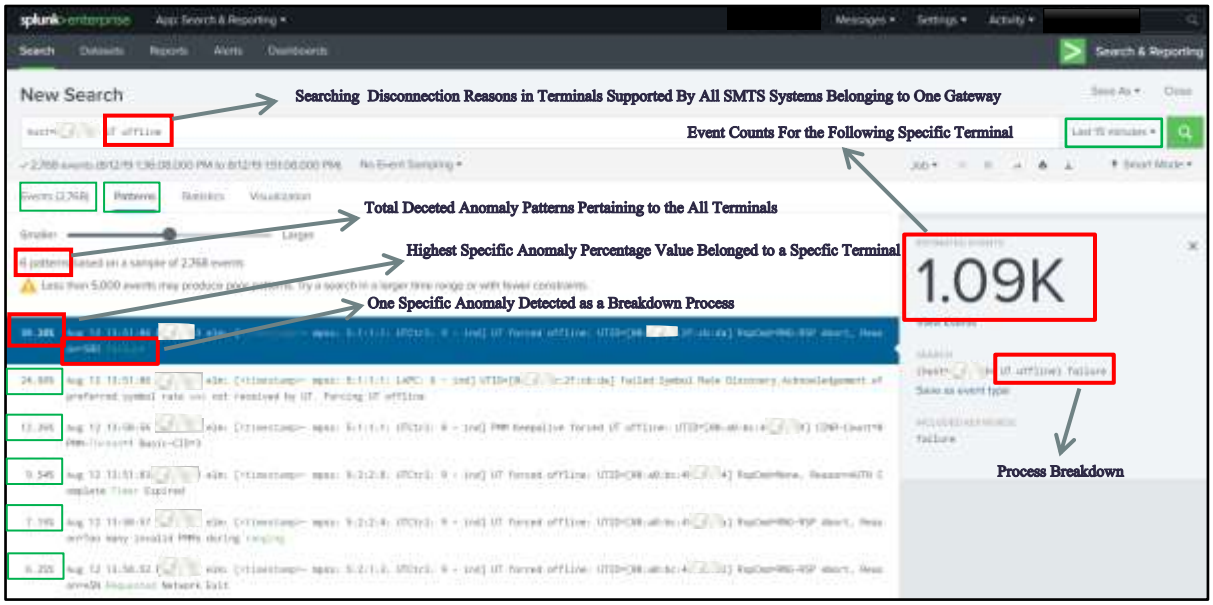


Figure 4.37: Illustration of Splunk anomaly detection based on pattern featuring

The rest of failures are occurred due to other reasons shown with their percentage values in KA-SAT platform. Following this, in next paragraphs, we will discuss and investigate the root cause about the most common occurred anomalies as critical use cases through the KA-SAT platform. Therefore, using this Splunk's capability makes a huge impact in terms of acquiring insights rapidly and realizing what is happening with the collected data and finally addressing that the occurred problem at once. By this, it is possible to imagine in an organization's sense perspective, if there will be a failure, anomaly, or any issue through monitoring services activities, then we are able to detect and identify in real-time the root cause in which specific area of the system happened and eventually performing necessary actions in order to resolve the problem or troubleshoot the failure to maintain the system operationally.

4.2.5. Monitoring and Alerts

Generally, monitoring and alerts are the most leading features in Splunk log analysis approach. Being able to make decisions proactively will make more this related business opportunities. Moreover, being able to understand what is happening with our data on getting the coming alerts which are notified by monitoring data activities and being able to fix and solve the crashes instantly will save a lot of time and costs and so with Splunk, we can monitor and respond to particular events in real-time or on a schedule-base and that is what the alerts do from various elements of KA-SAT platform in log format types. An alert trigger when specific search condition is met and to indicate one of the most known one is memory failure relating to the disk usage of one SMTS

system's component which is typically has three various status of warning, critical, and information level. Following this, when the percentage of used memory reaches or exceeds from defined threshold, relevant alerts will be triggered and in the worst case which is referred as critical status, SMTS system crash will be occurred and it impacts in delivering services toward to the terminals and they suffer a massive disconnection issue. Technically, when this failure event is happening, it must be considered as a high-priority event that should not be happening later. But when it happens, it is required to wait for a long time to handle the situation and inspect how the terminal interaction is failed. By using an enterprise tool properly and once implemented in our organization, we able to be step ahead of everything to perform real-time actions effectively to fix this crash. To imply another advantage of Splunk, it can be run in real-time for all daily time periods to troubleshooting and monitoring services and particularly it is so beneficial when we are in development of an event phase. Moreover, by using Splunk via monitoring the platform efficiently, we can find simply when an incident or crash occurs in the platform and it becomes very important to imply when the failure cost and downtime is widely large. As an example, the providing service is unavailable to access and it causes a massive drop in terminals to connect for long hours due to be a faulty component within the platform and this can result huge revenue lost for the satellite service provider. As a result, by deploying Splunk the root cause of the failure can be identified rapidly.

4.2.6. Visualizations and Reports

Splunk has the capability of doing visualizations as reports which contain useful information about the various areas of KA-SAT platform in different aspects. Through the Splunk analyzer various topics can be analyzed and examined as following items:

- **Heatmap trend display of entire SMTS systems crashes**

  This indicates a heatmap trend display to show the crash logs on the SMTS systems over time and correlate the events between the different SMTS systems belonging to total gateways in 30 days periods. As it is clear, we can see a large flood trend of crash logs on one SMTS system supported by its relevant gateway which results a link down issue due to occurring a failure on its component part and this case is specified in the figure 4.38. The most occurred crashes are on many SMTS systems on November 29th. In next paragraphs, we will discuss about the reasons and root causes as a use case term.

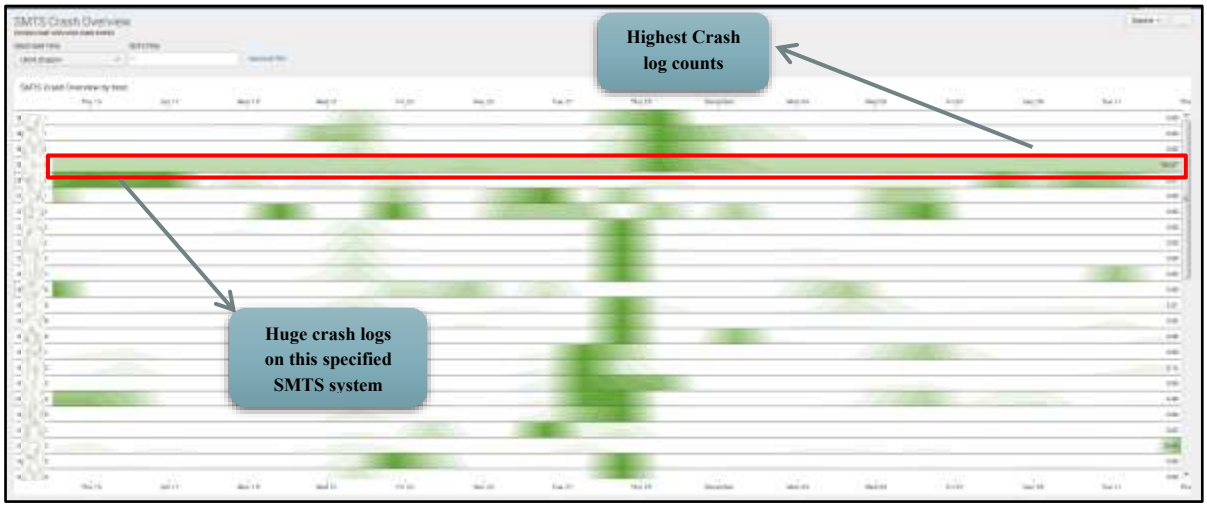


Figure 4.38: An Heatmap illustration in Splunk view

- **SMTS Crash events in Multi-chart view**
  Since each SMTS system has different components to perform relevant tasks and activities, a certain group of issues or anomalies might occur through delivering different services. As an explicit example, the following figure 4.39 displays the statistics of one SMTS system's component named Base switch in which this component becomes faulty due to specific reasons and following this occurred anomaly the link is down, and in this status, all the users suffer service outage. According to the figure, different SMTS systems belonging to their gateways are involved with this anomaly type in various time periods during month of July. Depending on the SMTS system and the service impacts, the amount of the occurred event numbers differs, and this is sorted in different colors for each SMTS system separately. Regarding the multi-chart view, a set of complete statistics is depicted in two varied graph types.

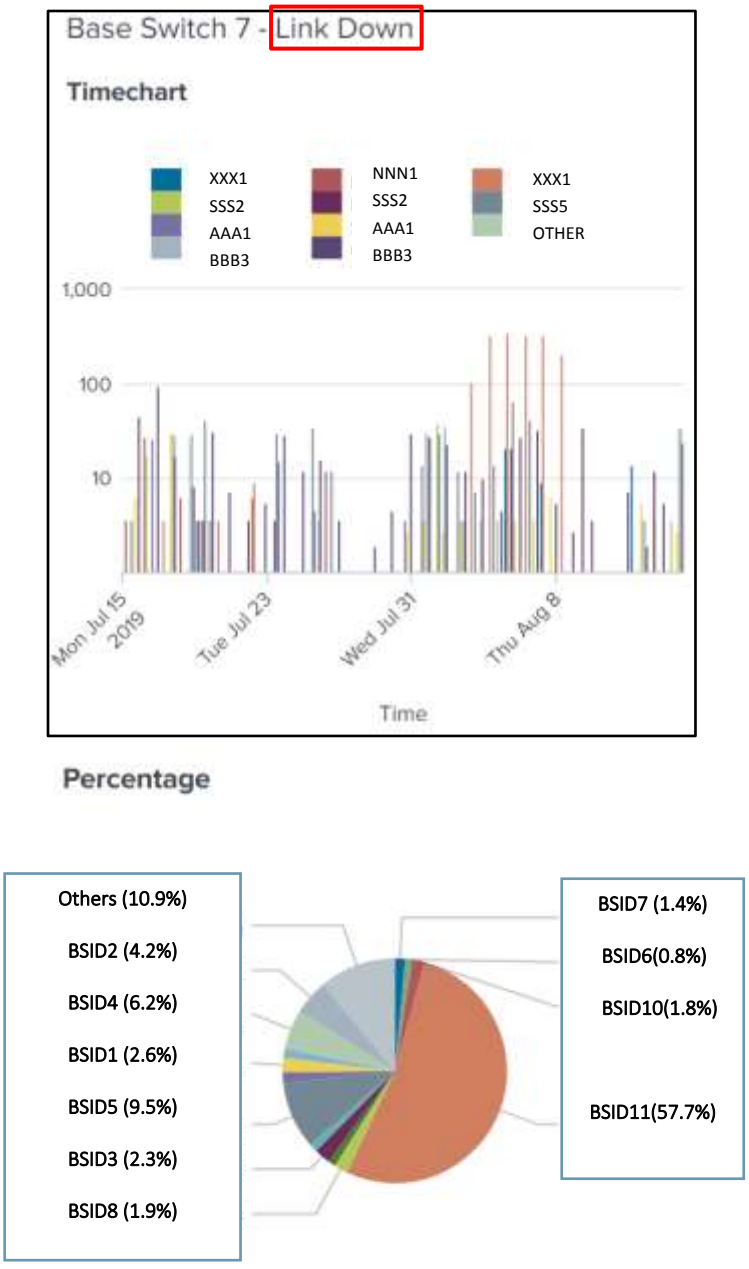


Figure 4.39: Crash statistics occurred in all SMTS systems over a definite time interval

Considering the visualizations and reports subject, the following Splunk interfaces are displaying the statistics relating to the crashes occurring in various SMTSs according to a definite time slot. Regarding the Offline SMTS dashboard in the figure 4.40, various user's disconnection reasons due to crash events are categorized including their reasons which are occurred in various areas of KA-SAT platform during certain specific processes and relevant histogram statistics are shown as well. These Splunk views are useful for monitoring activities and troubleshooting purposes.

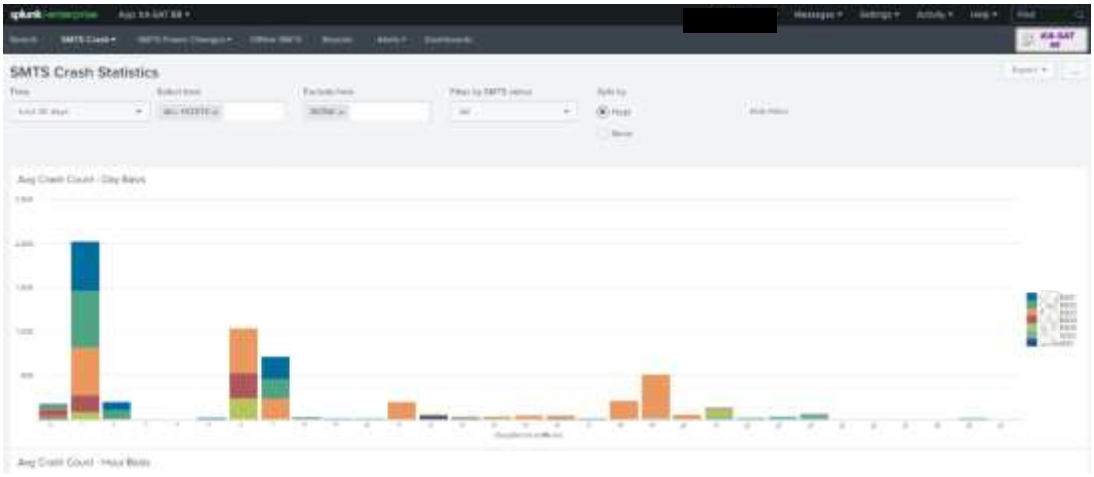


Figure 4.40: Illustration of SMTSs crash statistics which occurred over 30 days time period

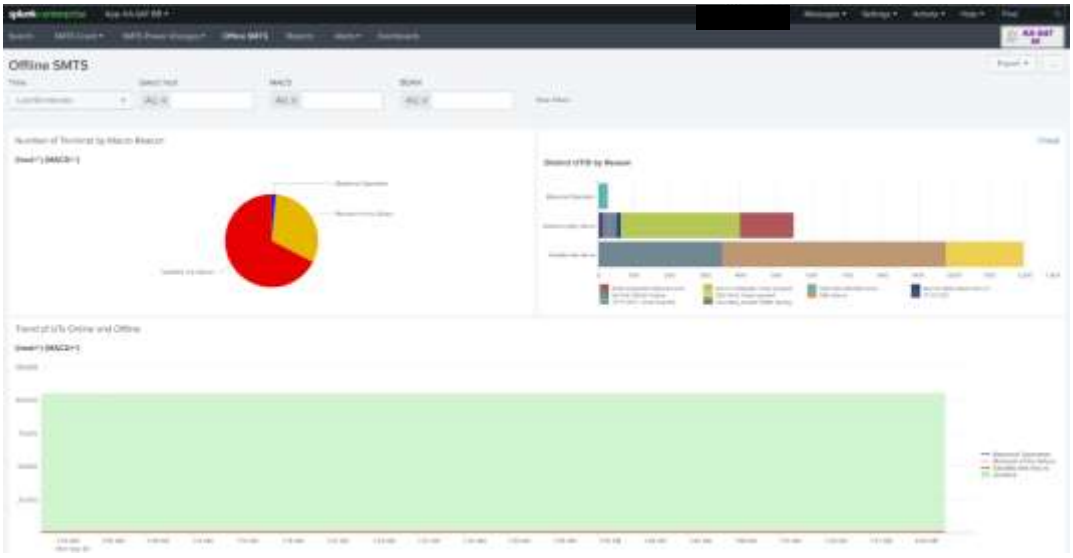


Figure 4.41: Disconnection reasons histogram statistics including its variant categorizations

The Splunk dashboard relating to the mobility service is depicted in the figure 4.42 and it includes information about various handover statistics which are carried out successfully or not.

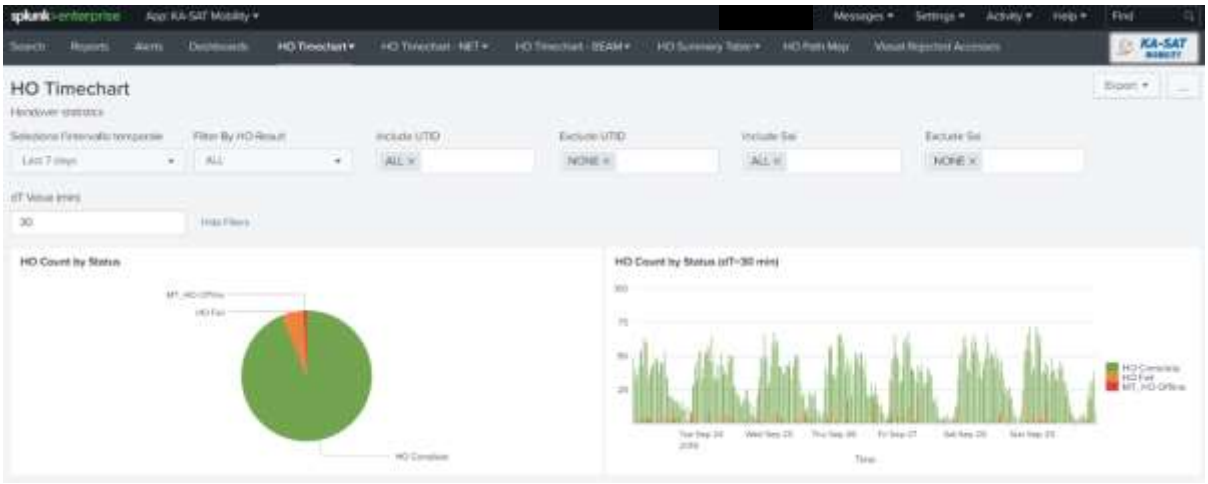


Figure 4.42: Splunk dashboard view of mobility service includes all histogram statistics

5. Experimental Method

The goal of this chapter is to present the experimental method which is referred as an investigation in order to explore the log analysis approach for event detection via Splunk expertise tool in KA-SAT platform during providing services. This investigation is exactly compliant with the attempts to identify the root cause of anomalies occurrence through KA-SAT platform. Initially, an overview of experimentation process is considered to perform. In log analysis approach exploration, Splunk enterprise tool is employed to analyze the log event elaborately and identify the root cause technically as well. Principally, the main goals of this contribution are to investigate, realize, and summate to the knowledge of log analysis capability for identifying the abnormal behaviors through the KA-SAT platform. In the following, all the phases are discussed respectively, and the experiment results are achieved by investigating of most common event use cases occurring on KA-SAT platform and eventually the dashboards are produced with log transaction to clearly and timely identify the root cause of the most common anomalies.

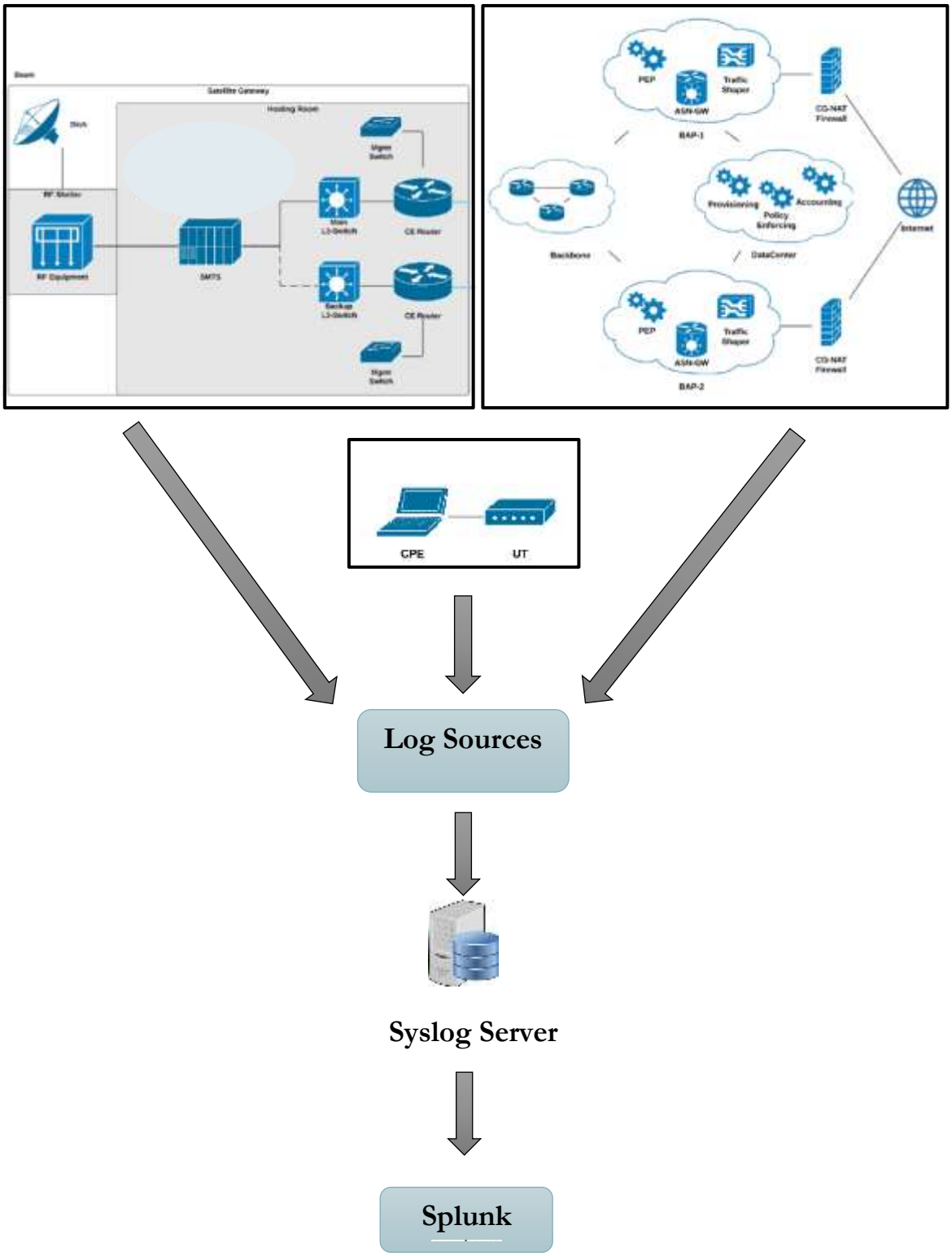
5.1. Experimentation process

The organized process through designing this experimental method is carried out form standpoint of log analysis concept utilization. This process comprises four major phases to perform. Regarding the phases of the following process, they are respectively including main network design scheme of the platform, identifying log analysis use cases, opted platform elements, and log analysis use cases implementation. All these described phases are designed aiming to employ log analysis approach over KA-SAT platform.

5.1.1. Network Design scheme

This phase is aiming to introduce the experimentation domains and network structure. This phase is designed in a high level of the network scheme in a way that it can evaluate and make a sensible result of employing log analysis approach by suing Splunk expertise tool and all the main elements and components of KA-SAT platform including data flow among the various elements are considered as well. The network structure composed by three main domains which consist of variant elements and entities in the main infrastructure such as networking and satellite gateway components and user equipment as well. From each component and element, all the specific source logs collected in a storage and centralized server which is called Syslog server, then it forwards all the logs to Splunk in order to visualize all required information in different areas pertaining to the main platform. In the experiment, the desired high-level network structure is considered as following design in figure 4.43.

Figure 4.43: Network structure used in experimental method [27]



5.1.2. Identifying Log Analysis Use Case

Regarding the adopting log analysis approach employed in KA-SAT platform, it would provide a better starting point for event detection by implementing it in our organization. In log analysis, the basic translation is considered as a use case and by defining such this use case, implementing, responding, and managing of it would become straightforward to do. Subject to this, the starting point would be defining a use case and executing its steps and then eventually fetching up with certain cases that will be discussed in next sections.

As described before, a use case introduced as an activity to perform as a rule or report targeting to solve the requirements depending on the organization objective. This use case includes certain phases which are referred as a complete development process methodology to be performed to satisfy organization's requirements and identify the same use case as well and is discussed in section 3.3.2 completely. In this phase of experiment, log analysis use case should be identified by an approach through KA-SAT platform based on described event decomposition technique and following introduced development process which consists of six steps. This derived approach is including 4 main phases to be performed targeting to identify the log analysis use cases based on use case definition concept in KA-SAT. These steps are explained as following major items:

1. **Requirement:** This phase is explaining what exactly required to be monitored in KA-SAT platform.

2. **Scope:** The scope definition phase should be introduced after requirement definition aiming to monitor and protect the variant elements and components through the main KA-SAT infrastructure.

3. **Event source list:** To list the event sources for applying the specific use cases on them in which the event logs pulled out from variant elements and components in KA-SAT infrastructure.

4. **Implementation:** The relevant tasks and activities should be implemented for following described use cases through KA-SAT platform.

Regarding this derived approach, the required and specific log analysis use cases which introduced for KA-SAT organization's requirements, they are described as following phases list respectively into two main types which are KA-SAT service platform monitoring and KA-SAT platform troubleshooting respectively. Both are shown in tables 4.2 and 4.3.

Log Analysis Use Case I: KA-SAT service platform monitoring

Use Case Definition Phases	Description
Requirement	• Monitoring anomalous event detection over delivering service through KA-SAT platform. This would generally mean the KA-SAT infrastructure that requires to be monitored and considered as a high priority for the peculiar requirement.
Scope Definition	• All KA-SAT infrastructure entities and customer premise equipment
Event Source lists	• Event log messages collected from various described platform elements forwarding to main syslog server: 1) Satellite gateway equipment (Satellite modem termination systems, Radio Frequency components, Switches, Routers) 2) Networking systems and devices (Core node, backbone and data center network elements and systems) 3) Customer premise equipment
Implementation	• Traffic rate monitoring for each gateway and core nodes at both satellite fixed and mobility services over forward and return transmission links • Operative and active status and main metrics monitoring and health checks for each device and system periodically such as average signal to noise ratio, forward link and return link congestion and efficiency, • Monitoring trend graphs of network devices and systems such as traffic rate and relevant criteria continually • Link capacity checks by monitoring the bandwidth usage of each circuit • Monitoring, adjusting, and implementing metrics of common mode frequency tracking (CMFT) algorithm periodically

Table 4.2**:** Log analysis use case definition phases

Log Analysis Use Case II: KA-SAT platform troubleshooting

Use Case Definition Phases	Description
Requirement	• Troubleshooting for occurred anomalous events and incidents through KA-SAT platform including both infrastructural elements and customer premise equipment
Scope Definition	• All KA-SAT infrastructure entities and KA-SAT customer premise equipment
Event Source lists	• Event log messages collected from various described platform elements forwarding to main syslog server: 1) Satellite gateway equipment (Satellite modem termination systems, Radio Frequency components, Switches, Routers) 2) Networking systems and devices (Core node, backbone and data center network elements and systems) 3) Customer premise equipment
Implementation	• Detecting root cause and diagnosing of occurred anomalies on KA-SAT platform in in real-time • Assessing device health and troubleshooting • Pinpointing scope of poor performance • Searching for user terminal activity through relevant events • Verify the service model at both fixed and mobility types aiming to improve the delivering service efficiently • Compensating and restoring to nominal values and metrics I case of any abnormal behavior for all parameters used in different entities

Table 4.3: Log analysis use case definition phases

5.1.3. Platform Elements and Entities selection

This phase of this experiment is pertaining to the various infrastructure elements and components at both logical and physical types which are required to implement log analysis use cases on them in KA-SAT platform. These are introduced as variant sources such as firewalls, access service network-gateway (ASN-GW), satellite modem termination system (SMTS), all internal and application servers, and switches and routers. According to the figure 4.43 which is introduced as a network structure in the experiment, all implied log sources such as platforms log messages and corporate network log messages are typically forwarded to the main syslog server and then will send to the Splunk server in order to visualize the results by Splunk presentation layer.

5.1.4. Log Analysis Use Case Implementation

This phase is verified completely by presenting and investigating three most common event use cases in which typically occur in the KA-SAT platform during delivering services by log analysis use case implementation. Practically, the real implementation of log analysis use cases will be performed and afterward, the derived investigated and resulted points will be shown as analysis information and dashboards in next sections. According to section 5.2.2 in which two leading log analysis use cases including their tasks and activities are discussed, various derived graphs used in KA-SAT platform in order to be monitoring KA-SAT service, are shown in the following figure as well.

Regarding the expressed log analysis use case concept through implementation phase of identification process in which certain tasks and activities must be performed as priority operations, the following important graphs must be continually monitored, and they are extracted from various areas of KA-SAT platform. These selected important graphs are targeting only for log analysis use cases which must be monitored continually or periodically to maintain the service operative.

The following sample graphs are related to the traffic rate of one gateway at both forward and return transmission links through delivering services to the users and this transmission rate assignment is based on the configuration of the gateway and total bandwidth capacity which can be supported by the gateway aiming to transmit to the beam and then forwarding to allocated users by supported beam coverage.

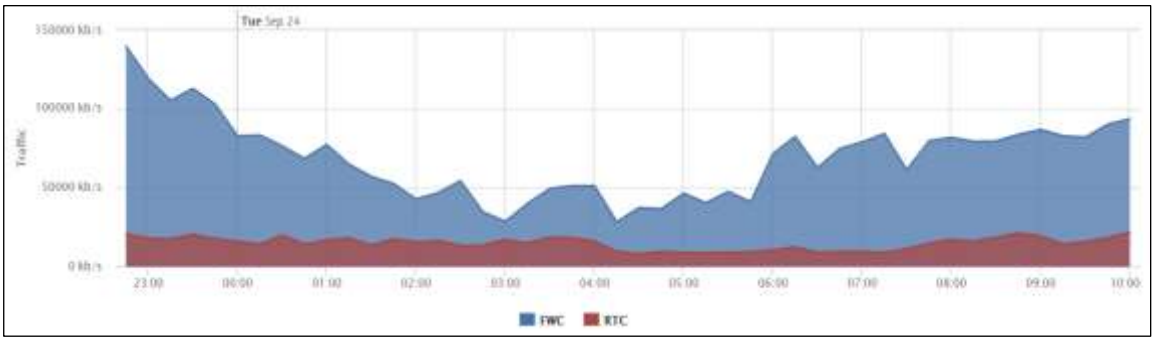


Figure 4.44: Gateway traffic rate at both forward and return transmission links

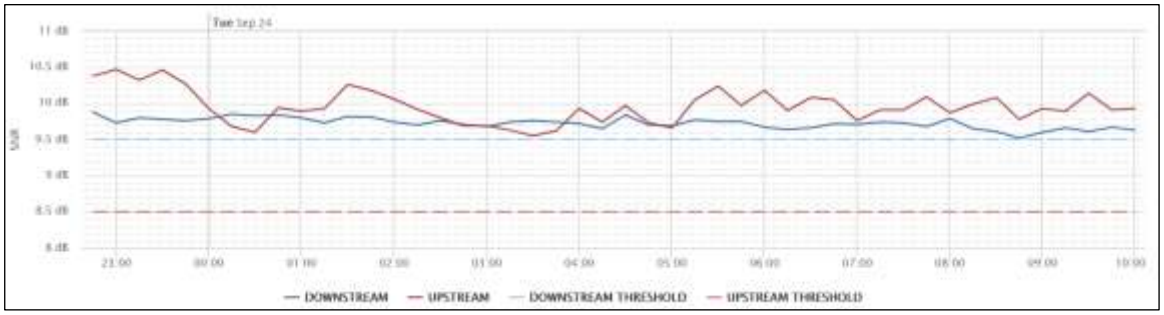


Figure 4.45: Gateway average signal to noise ratio for uplink and downlink plus thresholds

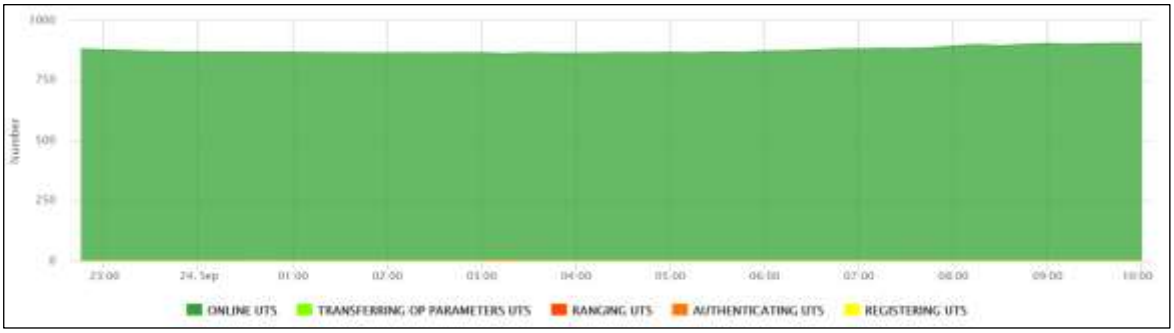


Figure 4.46: Terminals numbers supported by one beam plus terminal process types indication

Depending on the anticipated demand coverage for delivering services and bandwidth allocation for the users, the following figured graphs may vary in various parameters and user numbers.

In the following, the figured first graph is related to one beam traffic transmission rate supported by its relevant gateway comprising both forward and return transmission links. Moreover, next graphs are associated with signal to noise ratio through right- and left-hand circular polarizations within uplink and downlink paths and comprising their thresholds as well. Depending on weather conditions and any case of incident or anomaly, all these graphs impacted and suffer service degradation and outage which such these event types directly effect in providing service to all allocated users on this beam to become offline or low received power.

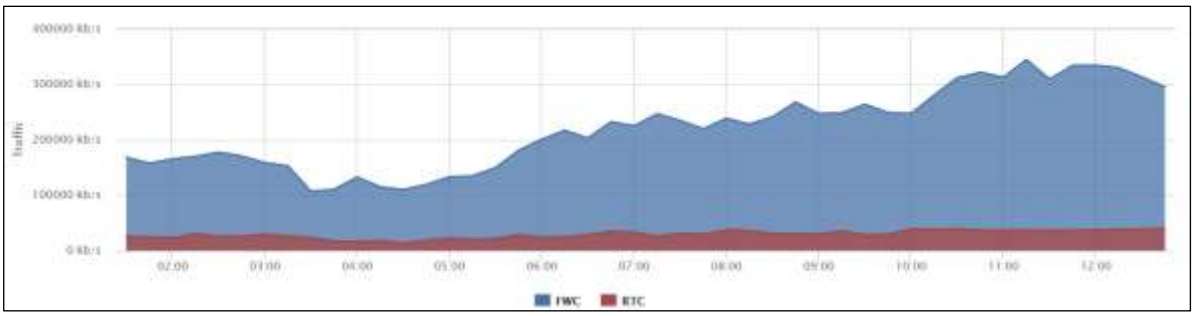


Figure 4.47: Beam traffic rate supported by gateway at both forward and return transmission links

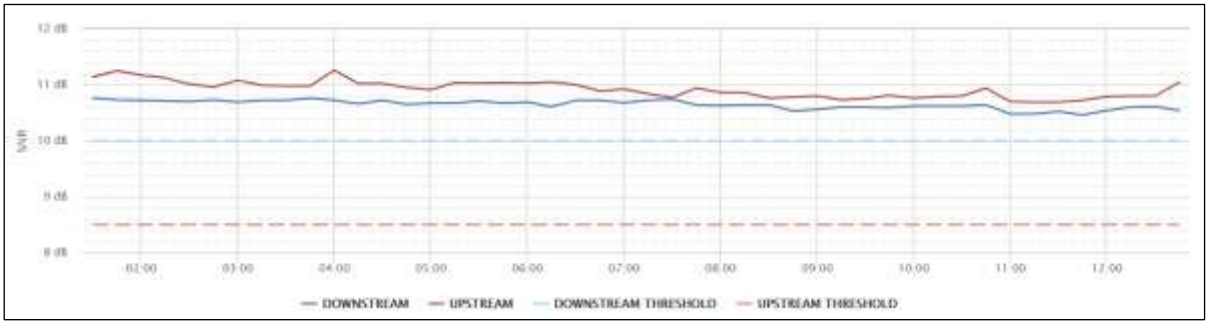


Figure 4.48: Beam average signal to noise ratio at both uplink and downlink plus thresholds

It is noted that depending on configuration and specifications of each gateway, the figured graphs may vary in various parameters, user bandwidth allocations, and user numbers as well.

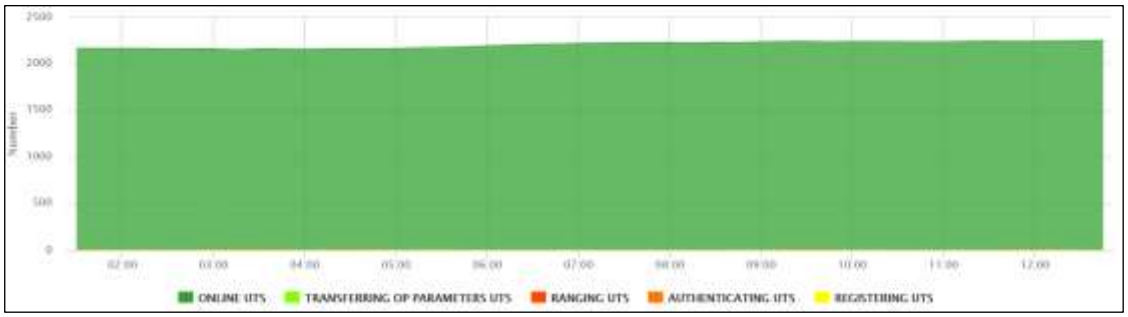


Figure 4.49: Terminals number assigned to one beam plus terminal process types indication

Following first graph is related to the whole online user counts which supported and allocated to satellite modem termination system (SMTS) and access service network-gateway (ASN-GW) through KA-SAT platform. The second graph is showing the common mode frequency tracking (CMFT) graph containing defined nominal curves ranging from minimum, average, maximum, and current values. As described before, this algorithm is used by SMTS in order to compensate the frequency error due to explained reasons. According to the figure 4.50 belonged to a sample beam, three described main CMFT parameters which are belonged to demodulators can be seen in the figure 4.51. Each parameter is used for a specific purpose which are used for return link, forward link and tracking in mixed populations environment, respectively.

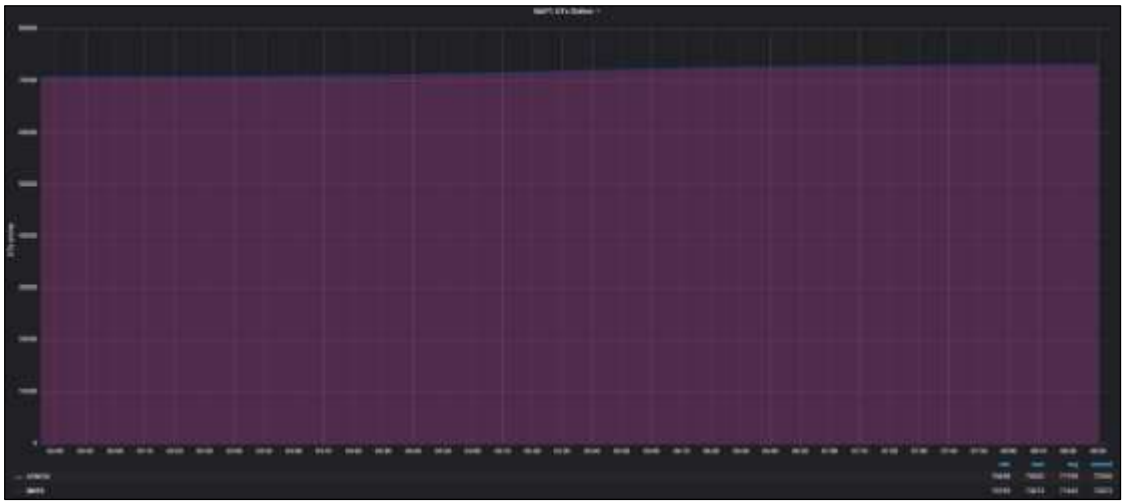


Figure 4.50: Online user count statistics allocated to SMTS and ASN-GW belonging to core node

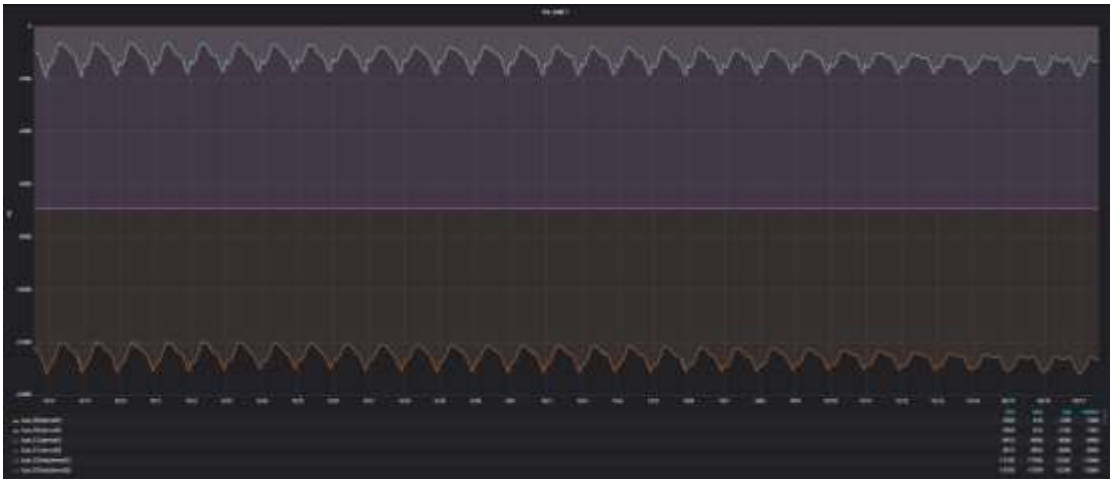


Figure 4.51: CMFT algorithm graph for a beam comprising its main parameters in various values

As implied before for previous indicated graphs, depending on the configuration and user and bandwidth allocation for each intended beam, the nominal value of each parameter may vary during delivering service.

5.2. Experimentation Results

Regarding the experimental method procedure, we are going to verify and investigate technically on expressed following abnormal behaviors elaborately introduced as significant anomalies and incidents which are typically occurring in the KA-SAT platform during delivering service at both fixed and mobility types. Afterward, the obtained results and observations will be provided by a comprehensive and elaborated analysis from investigated starting point to finalized results which will be displayed as dashboards aiming to assist and guide engineers and operators in various teams to detect the occurred event, identify the root cause, and perform troubleshooting for further events.

According to the all discussed various use case concepts such as use case definition, use case identification process, and log analysis use case implementation in the KA-SAT platform, this investigation and analysis are going to be performed as an experimental method on significant anomalies which are called as event use cases. For each event use case, elaborated and technical analysis including platform reporting graphs will be discussed and eventually dashboards based on described design process, will be represented in this section. In the following discussion, three most common anomalies as KA-SAT platform event use cases will be analyzed and investigated in which two use cases are fixed type and the other one is mobility type.

5.2.1. KA-SAT Platform Event Use Cases

This section is aiming to provide technical and investigational information about the most common incidents referring as abnormal behavior through KA-SAT platform. In order to verify these event use cases based on the described experimentation procedure, they are discussed in detail respectively in the following subsections.

5.2.1.1. Event Use Case 1: An RF Equipment Anomaly I

One of the most common platform anomalies is a block upconverter (BUC) component failure occurrence through the antenna radio frequency (RF) chain belonging to the ground segment platform in uplink transmission path towards to the terminals and this anomaly typically points out that the specific ground segment platform not working as usual full functionality and operative in uplink transmission path.

From technical point of view, block upconverter is used in the uplink transmission of satellite signals and is responsible for convert a band of frequencies from a lower frequency to a higher one. Each block upconverter operates in three different frequency bands and two polarizations including right-hand circular polarization (RHCP) and left-hand circular polarization (LHCP). In

KA-SAT platform, whenever a BUC failure operating on a specific polarization and frequency band occurs, it impacts remarkably on a great number of terminals allocated on variant beams and other elements including their relevant components as well.

In order to identify the root cause of one particular relevant event use case through the KA-SAT platform, the main focus attention on this investigation is on this such BUC anomaly which results massive drops on most terminals allocated on these two specific beams supporting by one satellite modem termination system (SMTS) system in right-hand circular polarization (RHCP) and these terminals typically suffer service outage. As described, this anomaly impacts on the other elements and their related components and creates problems in communication between the terminals and ground segment through variant processes targeting to make the terminals operational and online.

To describe deeply, ground segment typically communicates with all terminals by performing certain steps as exchanging specific messages periodically through the uplink transmission path aiming to determine the proper modulation, transmission power level adjustment, terminal online and operative status checks, bandwidth assignment, etc. Following this anomaly, when a BUC component operating on one polarization and frequency band becomes faulty, ground segment is not cable of communicating and exchanging messages with terminals periodically and this results communication outage and terminals cannot receive the service properly and works operatively as online status.

It is noted that in certain specific conditions, this is not caused to service disconnection completely towards to terminals and is considered as a service degradation issue which is also referred as a low SNR power level in forward transmission link, i.e., the link forwarding to the terminal.

Through the typical applied investigation, the problem is raised in RF chain through the block upconverter component which instability status founds in the output voltage of the local oscillator on the block upconverter system and by performing proper resolution referring as switchover operation to the spare block upconverter, the situation can be rolled back to the normal and operational status and this proposed resolution ensures the service stability and following that, all the terminals can become operative and online after resolving this anomaly.

Considering this anomaly and its extracted Splunk results, an explicit massive drop of terminals due to different reasons which caused by this anomaly can be noticed simply through the figures in below. Since, within ground segment platform, each gateway encompasses several SMTS systems and each one can typically support certain allocated beams, the aggregate average number of allocated terminals on following beams is reduced widely due to this anomaly occurrence. The aggregate average terminals uptime at both normal and anomalous conditions is shown in the following figures. In Splunk view, which is shown in figure 4.52, all important information and statistics are pointed and explained briefly in our search. According to this Splunk view, variant breakdown processes which cause to forcing terminals offline due this anomaly are extracted as reasons list containing counts and percent values. This list is depicted based on high to low counts and percentage within the figure 4.53.

Figure 4.52: Splunk dashboard with log analysis description illustration

As expressed, the bidirectional communication performed between the ground segment and terminals typically fulfilled via various fundamental processes and steps periodically and depending on the process even constantly targeting to provide service and maintaining the connection with terminals for all required criteria for verifying their status continually.

Figure 4.53: Processes breakdown list caused by the anomaly occurrence plus percentage value

All the indicated processes in the reason list which created and impacted by the following anomaly to force large amount of terminals in an undetermined time, are responsible to accomplish specific tasks between variant elements and entities in ground segment platform and terminals which are including processes and steps as network entry procedure, physical layer adjustments, initial communications for return link bandwidth allocation, synchronization, power level corrections and adjustments, digital signal processing techniques to determine the symbol rate, forward and return link bandwidth scheduling, frequent operative status checks of terminals, and etc.
It is noted that all these processes and operations are performed between ground segment platform elements and each terminal via negotiations and sending-receiving requests and responses as following diagram:

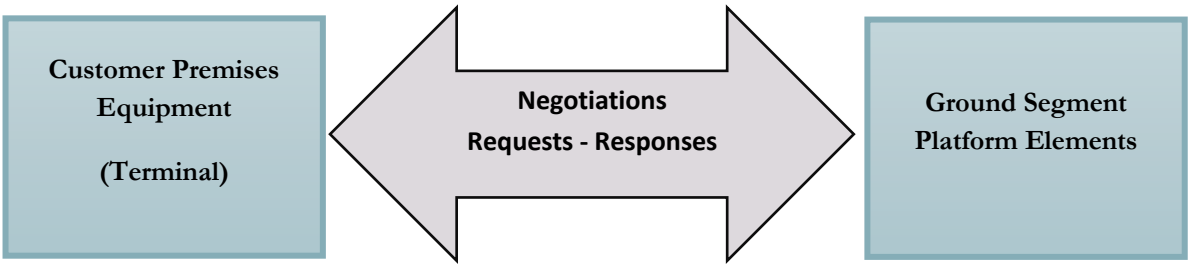


Figure 4.54: Typical contacts between terminal and ground segment platform elements

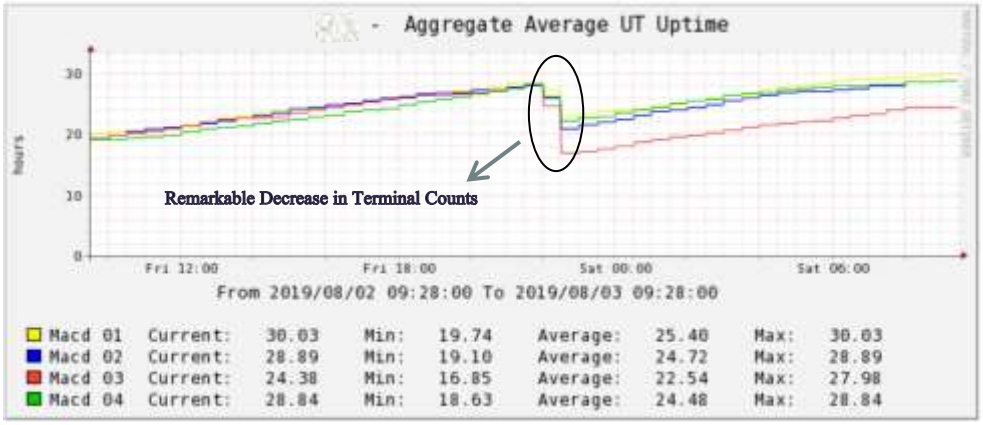


Figure 4.55: Reduction in the average number of the terminals allocated on indicated beam

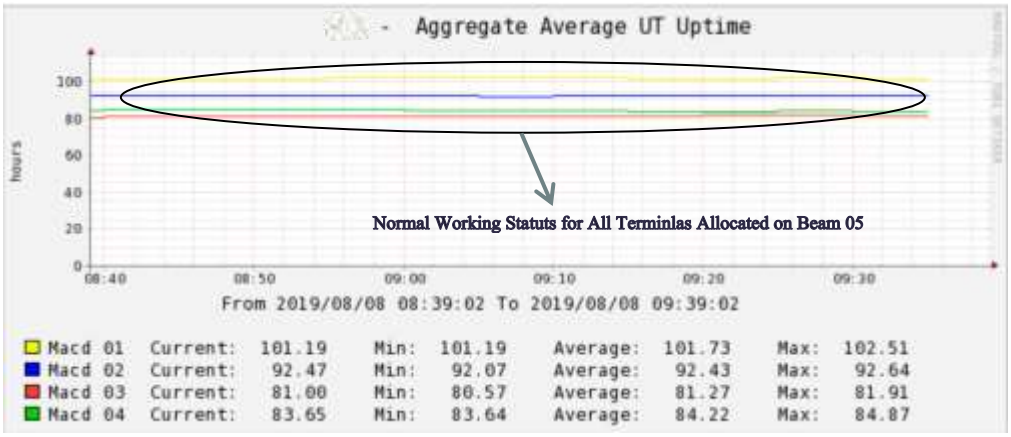


Figure 4.56: Normal status of the average number of the terminals allocated on indicated beam

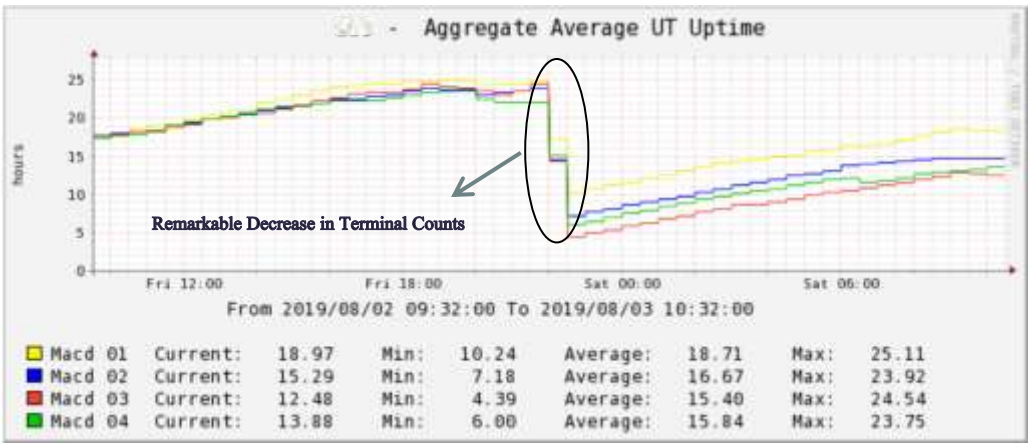


Figure 4.57: Reduction in the average number of the terminals allocated on indicated beam

Regarding this anomaly and its impacts, variations in average number of terminals allocated on introduced beams are shown in the figures 4.56 and 4.57. In addition, the average number of terminals allocated to typical beams are depicted in figures 4.56 and 4.58 as normal and operational status.

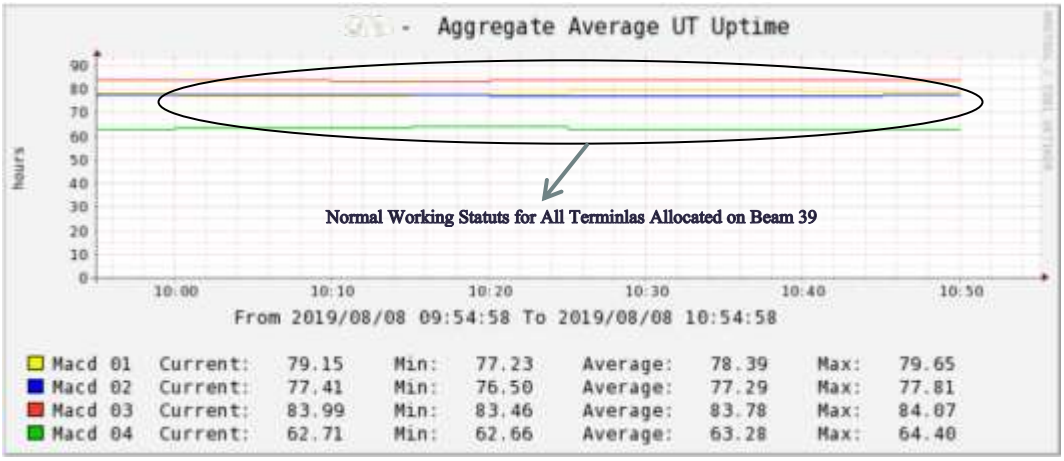


Figure 4.58: Normal status of the average number of the terminals allocated on indicated beam

Regarding this anomaly, the following dashboard design displayed in figure 4.59 that indicates variant disconnection reasons analysis of user terminals through KA-SAT platform. Furthermore, the online and offline trend of users plus their count statistics are displayed.

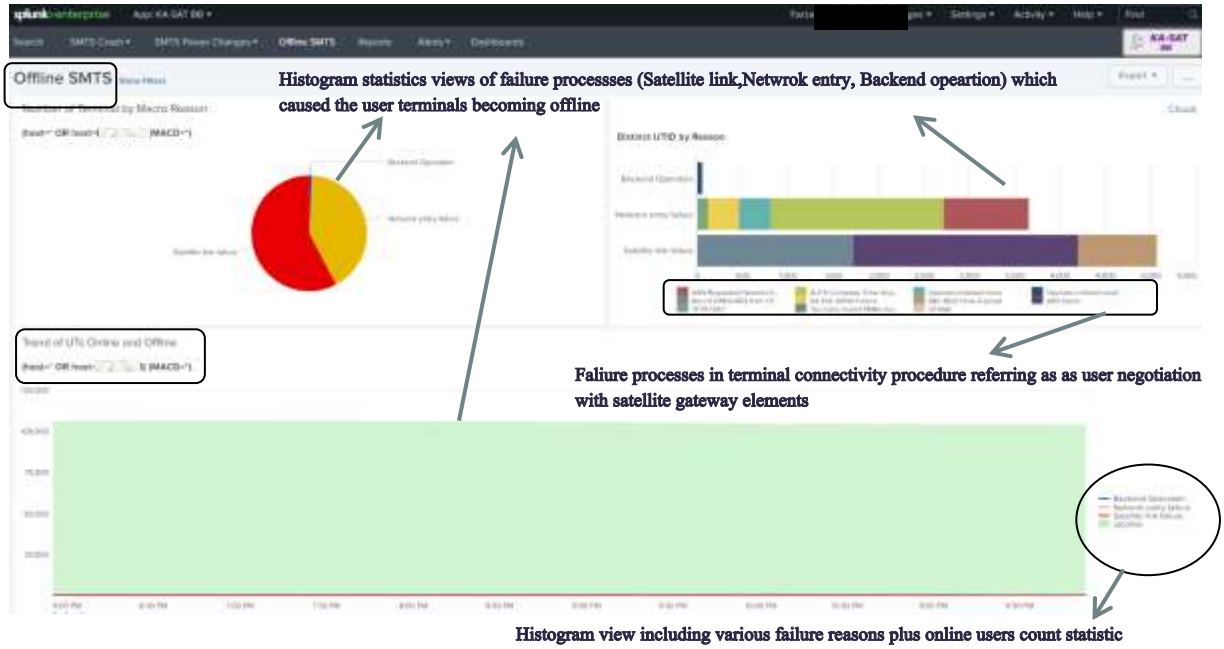


Figure 4.59: KA-SAT fixed dashboard view

5.2.2.2 Event Use Case 2: An RF Equipment Anomaly II

To introduce another most common anomaly occurrence in the KA-SAT platform through the radio frequency (RF) chain, is a block downconverter (BDC) component failure introduced as an anomaly which impacts remarkably on a large number of terminals allocated on beams supporting by its relevant satellite modem termination (SMTS) system through the related ground segment platform and this certainly creates a massive drop for majority of terminals to force them becoming offline. This issue is also referred as communication outage particularly in return link referring as downlink path between the terminals and Earth station points.

The BDC component placed at radio frequency chain within the ground segment platform through reception segment operating in downlink transmission path. In general, this converter is responsible for converting a band of frequencies from a higher frequency to a lower frequency. From technical standpoint, it serves as RF front-end of the satellite receiver, receiving the signal from the satellite collected by the dish antenna, and then amplifying it.

Technically, each BDC component operates in three variant frequency bands and depending on which BDC component in the radio frequency chain, each one operates separately in right-hand circular polarization (RHCP) or left-hand circular polarization (LHCP) through the downlink transmission path which is referred as return link, forwarding from a specific terminal and receiving by the satellite gateway. Since each SMTS system is placed at ground segment platform, it typically transmits and exchanges specific messages continually with the terminals to perform certain required processes in order to maintain the connectivity and provide service properly as well.

When a BDC component operating on one polarization and frequency band becomes faulty, the communication between the terminal and ground segment might be impacted and depending on the intensity of the anomaly, it may cause massive drops for a great deal of terminals allocated on one or more specific beams in which they are not able to communicate with the Earth station in return link path and as implied before, this is referred as communication outage as well due to being terminals offline.

Considering this anomalous condition, various forcing offline reasons during accomplishment of processes can be extracted from this anomaly occurrence. According to the figure 4.60, which is a Splunk view of such this anomaly, all the relevant event logs and statistics are available to notice. Regarding this component anomaly, remarkable number of terminals are forced to become offline and they cannot communicate with the relevant ground segment due to variant reasons. This anomaly certainly impacts on the other elements in which through this case, one related beam including allocated terminals are impacted and following anomaly makes certain problems through various processes fulfilment through terminals to perform required steps to become online and receive service properly. These impacts which are resulted by this anomaly referring as variant processes breakdown are shown and listed in the following Splunk interfaces referring as reasons to compel the terminals to become offline.

Thus, in order to find the root cause, by searching following query activity through the Splunk view, all information and statistics extracted aiming to simplify the root cause identification for resolving and troubleshooting the various inferred process breakdown cases targeting to restore

all the elements operationally. Resulting these actions and operations would be delivering service towards to the terminals properly and they come back to normal status to be online.

Figure 4.60: Splunk dashboard with log analysis description illustration

As described in previous investigated event use case, certain basic processes and steps must be fulfilled based on diagram in the figure 4.58, referring as communication between terminals and ground segment aiming to delivering service and other fundamental purposes such as determining forward and return link modulation, power level adjustment, continual terminal online and operative status checks, etc. All these processes breakdown containing counts and percentages are shown as reasons list in figure 4.61.

Figure 4.61: List of processes breakdown which caused by the anomaly occurrence

Considering this anomaly occurrence, the following dashboard design displayed in figure 4.62 which indicates variant disconnection reasons analysis of user terminals on the KA-SAT platform. Then, the online and offline trend of users plus their count statistics are shown as well.

Figure 4.62: KA-SAT fixed dashboard view

Regarding the anomaly occurrence, a massive and remarkable reduction through the aggregate average terminals uptime allocated on a specific beam can be noticed in the figure 4.63 explicitly. Furthermore, the normal condition of the implied aggregate average on the following beam is depicted in figure 4.64.

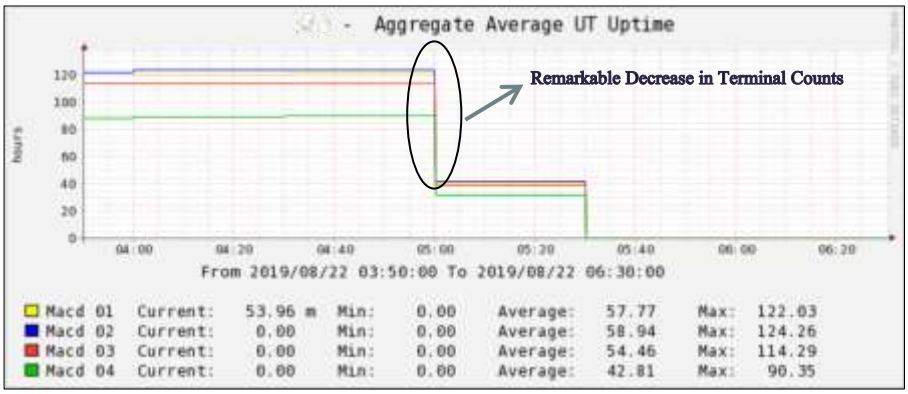


Figure 4.63: An explicit reduction in the average number of the terminals allocated on indicated beam

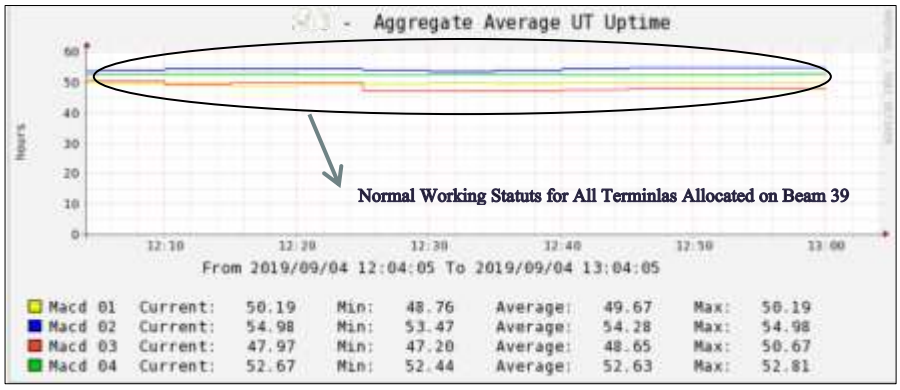


Figure 4.64: Normal status of the average number of the terminals allocated on indicated beam

5.2.2.3. Event Use Case 3: Mobility Handover Anomaly

This mobility manager event is considered as an anomaly occurrence through KA-SAT mobility services at which the process is not accomplished successfully and is called handover failure. As described in section 2.2.4, the handover technique is managed and directed by mobility manager entity for all mobile terminals in the KA-SAT platform. The handover procedure is performed by communicating as exchanging end-to-end messages using radio resource manager (RRM) interface between an SMTS system and the mobility manager entity in order to comply the mobility terminal request based on being a maritime or an aeronautical user type aiming to maintain the service accessible and available provided from current serving satellite beam to the target satellite beam without any interruption and loss in delivering service and eventually the handover process will be performed successfully and technically, this status is called handover complete.

Considering this, there are various anomalies relating to the handover failure subject which occur occasionally in performing handover process within different elements of the main network which results different anomalies such as massive disconnections in mobile terminals. This event use case is aimed to be investigated as an important anomaly in which resulting massive lost connectivity for the various mobile terminals types when they enter the target satellite beam coverage.

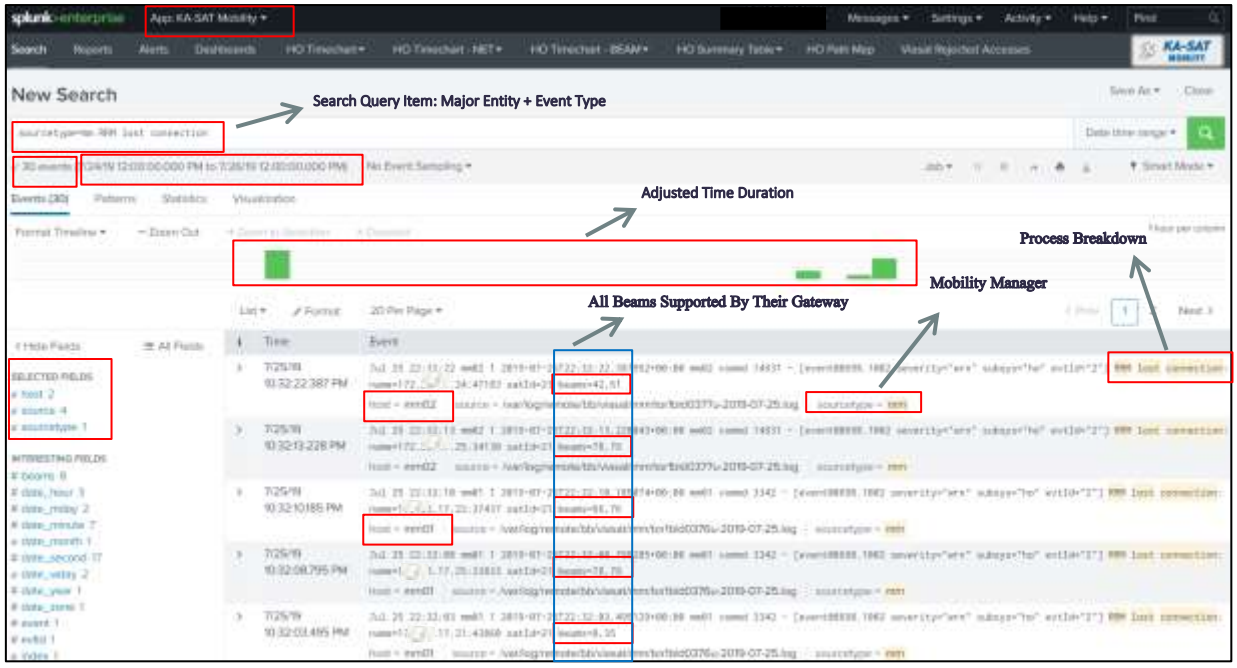


Figure 4.65: Splunk dashboard log analysis description illustration for KA-SAT mobility service

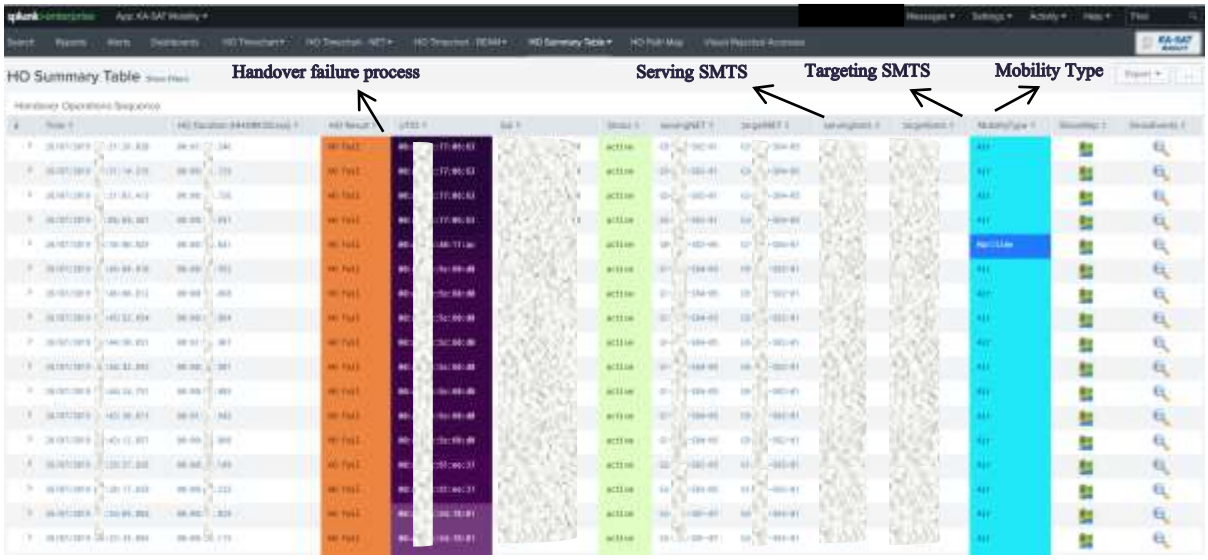


Figure 4.66: Splunk dashboard of KA-SAT mobility service for Handover failure process

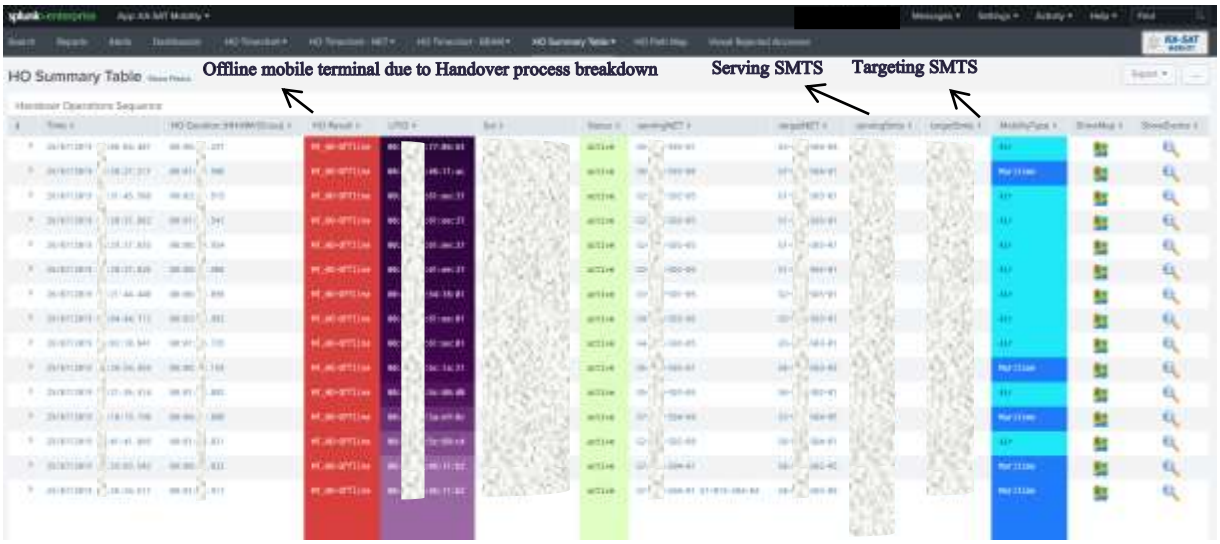


Figure 4.67: Splunk dashboard of KA-SAT mobility service for offline mobile terminal

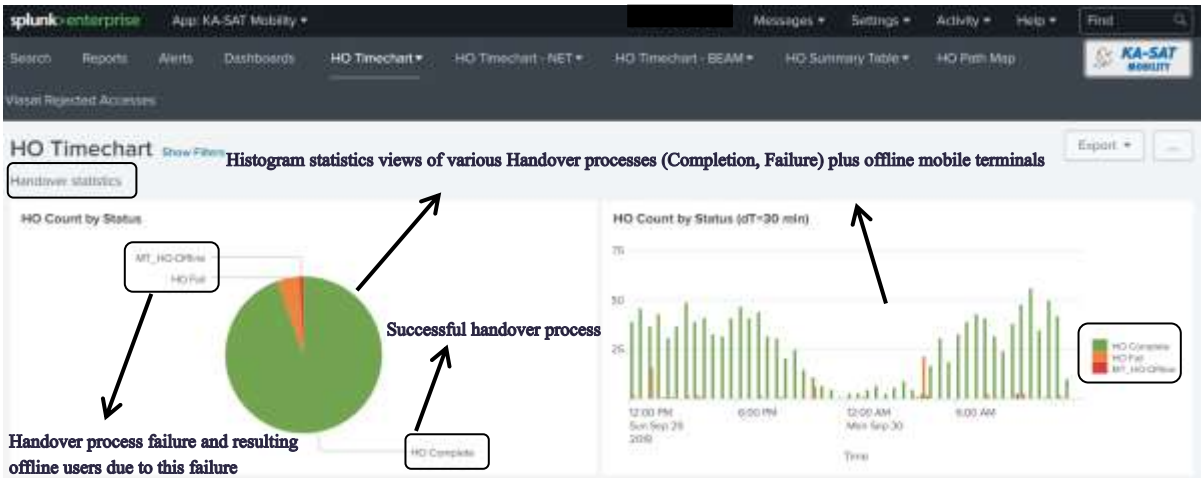


Figure 4.68: KA-SAT mobility dashboard view

According to the figures of 4.65, 4.66 plus figure 4.67, Splunk dashboard with log analysis GUIs including their descriptions are derived according to the handover failure process and offline terminals statistics. Eventually, regarding this anomaly and its analysis, KA-SAT mobility dashboard view is obtained and is depicted in the figure 4.68.

Part V.

Conclusion

6. Conclusion and Future Works

Based on my analysis, these described dashboards for both fixed and mobility will be employed by monitoring engineers to have a better utilization, providing accurate resolutions to troubleshoot in case of occurring any crash or incident.

This thesis presented an investigation of log analysis for event detection suited for most event use cases on KA-SAT platform during delivering broadband services. Particularly, it took into consideration log transactions for event detection case by using log analysis approach applied as an experimentation to this investigation. It is noted that the proposed methodology and analysis which have been exemplified on peculiar interest areas of KA-SAT ground and user segments, it is more adaptable and feasible in general to any purposes where analyzing and detecting can be advantageous and useful to identify more effectively the anomalies occurring on KA-SAT platform. Moreover, this study is more practical than theoretical, but theoretical approach is used to complement the practical part richly. Without doubt, satellite operators are attempting to improve their offering services excellence to the all various customer types throughout the world, and by using the latest technologies, they can benefit as well in particular for our case, effectiveness improvement of the troubleshooting actions to maintain the service available and reliable. Explicitly, the objective of this thesis is to simplify the root cause detection, by automating the log analysis for the most relevant event use cases, which linking the trigger logs to the outcomes occurred.

The method which is used for investigation is based on an experimentation which uses four main phases introduced as a network design scheme of platform, log analysis use cases identification process, platform elements selection, and implementation of log analysis use cases, in order to employ the described log analysis approach through KA-SAT platform. This is designed in accordance with KA-SAT organization requirements to boost troubleshooting activities and identify more effectively the anomalies and failures occurring over the platform and resulting this would be detecting the root cause rapidly plus automating the log analysis.

Various experiment results are achieved as variant dashboards plus analysis views by applying technical investigations of most common event use cases both for real-time anomalies and past events. In addition, Splunk expertise monitoring tool has been used for the analyzing and detecting at this study.

The current proposed method can successfully check and verify firstly KA-SAT infrastructure elements and entities in real-time during monitoring KA-SAT service. Based on the obtained results of this work, possible future directions can be reached as using this method to detect and identify the anomalies or failures during providing services occurring in different KA-SAT platform areas and based upon the gained information through automating log analysis for the most relevant use cases, technical root cause detection will be done simply and rapidly without spending more time. Ultimately, this leads to improve the effectiveness and efficiency of the entire troubleshooting activities and actions for KA-SAT fixed and mobility services. Following this, in

order to have a better understanding of this method to detect and identify the anomalies, a practical example is provided in the following paragraphs.

In a general case, in case of occurring an anomaly through the platform, firstly due to this anomaly, depending on its priority level, related event warnings are typically produced in high or low counts and then they will be monitored by the operators in order to check. Afterwards, the root cause of this incident must be identified and investigated technically by employing Splunk analysis tool and in addition, it is possible to check and monitor that how many and where the event logs are generated due to this incident by this expertise tool. Thus, according to the obtained results from Splunk plus relevant event logs trend statistics, they will be categorized in terms of which areas of KA-SAT platform becomes involved and eventually by providing technical resolutions and accomplishing required actions in order to troubleshoot this issue, the service will be provided properly as normal status.

To introduce another case, triggering an issue in the network provider links from the datacenter to other gateway through the terrestrial backbone infrastructure which is referred as service degradation may cause a reduction of the total amount of traffic to the user terminals and by the proposed method in the thesis, this can be automatically identified and detected and will be resolved and troubleshooted by gateway switchover operation to another backup gateway in order to maintain the service available and accessible for all supported user terminals by the primary gateway.

Furthermore, to propose a method that can be useful in improving effectiveness of the troubleshooting actions, is to carry out based upon the following proposed diagram in below:

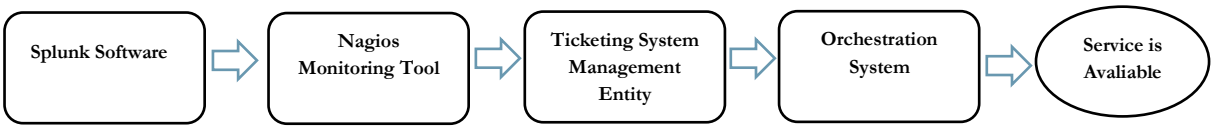


Figure 4.69: Diagram of proposed method

To describe each phase, in case of occurring an anomaly, the anomaly root cause can be identified by detecting the pattern event logs through Splunk expertise software. Then, an event warning will be generated as an event alert generator in Nagios monitoring tool in order to inform the operators. Following that, depending on KA-SAT platform area involvement, the event warning will be categorized through the ticketing system management entity as a ticket to rise. Afterwards, using orchestration system to orchestrate operational common activities for handling the most complex processes and applications integration. This would be advantageous in terms of time saving which means the issues and requests will be handled at machine, not human, i.e. it takes lower time to acknowledge to complete an activity. Moreover, it is hand-off-based approach which implies that there is no longer required to any operator to handle repetitive tasks and this allows

to operators focusing on important and complex tasks. The human errors would be reduced by executing workflow via machine. Eventually, by pursuing this proposed method and its procedure, in case of any abnormal behavior in the platform, the service will be operative and available rapidly as its normal delivering status.

In conclusion, regarding the method proposed in this thesis, all these mentioned procedures will be possible to carry out automatically from triggering logs step point to resolution phase and this certainly simplifies the root cause detection in real-time phase plus troubleshooting actions with time saving, no human error, and less human effort as well.

6.1. Limitations

Regarding this experimental method, the log data of the most elements and entities of KA-SAT infrastructure have the capability of forwarding to Syslog server via described procedure and then eventually Splunk server will receive all these log data. By referring to these log data via Splunk, the analysis and root cause identification for any occurred abnormal behavior will be carried out simply in order to resolve and troubleshoot the incoming and upcoming anomalies.

Due to some limitations through certain devices and components in RF equipment chain, it is not always possible to integrate logging for all the components, as they have various capabilities and support different protocols as well, but we can try cross-check other network components (such as SMTS system) in order to provide the same results that we are interested to obtain. Subject to this, for the future, we can additionally evaluate implementing a script aiming to connect to Nagios monitoring tool and afterwards generate logs about RF chain components, thus to have all the devices generating the event logs (even if it is not carried out directly).

Bibliography

[1] Satellite Communications Systems Engineering, Louis J. Ippolito, Jr. 2017

[2] Kepler's laws of planetary motion, https://en.wikipedia.org/wiki/Kepler%27s_laws_of_planetary_motion

[3] Broadband Satellite Communications for Internet Access, Sastri L. Kota, Kaveh Pahlavan, Pentti Leppanen, 2004

[4] Satellite networking, Principle and Protocols, Second Edition, Zhili Sun, University of Surrey, 2005

[5] Earth Segment Subsystem, https://www.tutorialspoint.com/satellite_communication/satellite_communication_Earth_segment_subsystems.htm#

[6] The Satellite Communication Applications Handbook, Second Edition, Bruce R.Elbert, 2004

[7] Future High Throughput Satellite Systems, Hector Fenech, Senior Member, IEEE, Alessia Tomatis, Sonya Amos, Viphakone Soumpholphakdy, Dimitri Serrano-Velarde, 2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL), Year: 2012 | Conference Paper | Publisher: IEEE

[8] Next Generation High Throughput Satellite System, O. Vidal ; G. Verelst ; J. Lacan ; E. Alberty ; J. Radzik ; M. Bousquet, 2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL)

[9] KA-SAT, URL, https://en.wikipedia.org/wiki/KA-SAT

[10] 5G mobile technology: A survey, Rupendra Nath Mitra, Dharma P. Agrawal, Department of EECS, University of Cincinnati, OH, USA, 22 January 2016, ScienceDirect, ICT Express 1 (2015) 132–137

[11] The role of satellites in 5G, Barry G. Evans, 2014 7th Advanced Satellite Multimedia Systems Conference and the 13th Signal Processing for Space Communications Workshop (ASMS/SPSC), 23 October 2014, IEEE, Italy

[12] High throughput satellites in 5G and MIMO interference limited Communications, Ana Pérez-Neria, Miguel A. Lagunas, and Miguel A. Vázquez, 1CTTC, Centre Tecnològic de Telecomunicacions de Catalunya, 08860 Castelldefels, Spain UPC, Universitat Politècnica de Catalunya, 08034 Barcelona, Spain, MATEC Web of Conferences, 76, 03008 (2016), CSCC 2016

[13] https://www.viasat.com

[14] O. Sallent, J. Perez-Romero, R. Agusti, and F. Casadevall. Provisioning multimedia wireless networks for better QoS: RRM strategies for 3G W-CDMA. IEEE Commun. Mag., 41:100–106, 2003

[15] J. Zander. Radio resource management in future wireless networks: requirements and limitations. IEEE Commun. Mag., 35:30–36, 199

[16] N. Dimitriou. Network planning & resource management issues for mobile multimedia CDMA systems. In IEEE 59th Vehicular Technology Conference, 2004. VTC 2004-Spring, May 2004

[17] https://www.splunk.com

[18] Thesis, Understanding Data Analysis Activity via Log Analysis, Sara Alspaugh, Electrical Engineering and Computer Sciences University of California at Berkeley, August 3, 2017

[19] Anton A. Chuvakin, Kevin J. Schmidt, Logging and log management, the authoritative guide to understanding the concepts surrounding logging and log management, Syngress (2012), 2013 Elsevier

[20] Learning Nagios: Edition 3 Wojciech KocjanPiotr BeltowskiAugust 31, 2016
Packt Publishing Ltd

[21] Nagios XI, Enterprise Server and Network Monitoring Software, https://www.nagios.com

[22] Use Case Analysis, SEEM, 3430 Tutorial, http://www1.se.cuhk.edu.hk

[23] Systems Analysis and Design, Use Cases, CSCI 375, http://www.csci.viu.ca

[24] Systems Analysis and Design in a Changing World, John W. Satzinger, Robert B. Jackson, Stephen D. Burd, 2016

[25] Identifying User Stories and User Cases, Event Decomposition Technique, https://www.jdatalab.com/

[26] Noetix, Dashboard, Dashboard Development and Deployment, A methodology, https://www.noetix.com/

[27] KA-SAT Services Documents, Architecture Overview, https://www.eutelsat.com/

[28] KA-SAT and Future HTS Systems, Dr. H. Fenech, Amos, Tomatis & Soumpholphkakdy, Future Satellite Systems, Eutelsat

[30] KA-SAT, High throughput telecommunications satellite, https://en.wikipedia.org/wiki/KA-SAT