Addis Ababa University

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

Short Message Service Fraud Mitigation Taxonomy: The Case of ethio telecom

By

Tarikua Worku

A Thesis Submitted as a Partial Fulfillment of the Requirements for the Degree of Master of Science in Telecommunication Engineering

Advisor: Dr. Mesfin Kifle

November 2018

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

Telecommunication Engineering Graduate Program

Approval of the Thesis Submitted By

Tarikua Worku

Thesis Title: Short Message Service Fraud Mitigation Taxonomy: the case of ethio telecom

Date of Submission: November 19, 2018

The final reading approval of the thesis was granted by:

Chairman, School Graduate Committee	_____ Signature
Mesfin Kifle (PhD) Advisor	_____ Signature
Surafel Lemma (PhD) Evaluator	_____ Signature
Ephraim Teshale (PhD) Evaluator	_____ Signature

Abstract

Telecommunication fraud is remaining challenging since the beginning of commercial telecom service. There are various reasons that makes telecom fraud mitigation inefficient. Some of them are; integration of new technologies without evaluating the security hole, lack of knowledges on the fraud root causes, the changing behavior of fraud and effective use of mitigation techniques. Short Message Service (SMS) is one of the main and victim telecom services. A variety of technologies, services and actors are involved on SMS ecosystem. This technology diversity makes the service vulnerable for different type of messaging frauds.

In this study SMS fraud mitigation taxonomy is proposed to improve fraud mitigation deployment method. The taxonomy is constructed from four main nodes namely Technology (Which), Vulnerability (Where), Fraud (How) and Mitigation (What) as a cause and effect way. These main nodes are also categorized in to three sub technological layers which are network/protocol, service and actor. In addition to this classification the mitigation techniques are characterized as technical and none technical.

The evaluation process is done first selecting 100,000 fraudulent short message records from ethio telecom. Then taking appropriate mitigation techniques from Network /protocol, Service and Actor layers. Finally, the selected records are examined by each layer mitigation techniques based on the fraud scheme.

The layered evaluation result confirmed the proposed approach can mitigate 70% of the fraud messages at network and protocol level, 57.2% at service level, and 84% at actor level before any impact. So that overall efficiency of this taxonomy based layered mitigation approach is recommended to use, instead of detecting the fraud after impacting the service.

Keywords: Taxonomy, SMS fraud, Mitigation techniques, Technology, Vulnerability

Acknowledgement

Above all, my gratitude goes to the almighty GOD, to give me the strength and be with me all times and will always be.

I would like to thank AAIT School of Electrical and Computer Engineering teachers and management for your effort to make this program happened and, I would like to thank ethio telecom to give me this chance.

I am also thankful to my respected advisor Dr. Mesfin Kifle for his invaluable advices. His dedication and willingness to discuss in any new ideas are always inspiring me as a model to follow in my future work and study.

I am also indebted to all instructors who support me while my education period, and I would like to thank IT Fraud Operation, Revenue assurance, Core network, signaling network, and Roaming and Interconnect staffs of ethio telecom. For their support in sharing valuable experiences, and for their welcoming approach.

Last but not the least I want to thank my beloved Mother, Child, Sisters and friends who inspire me while I am working.

Contents

List of Figures

List of Tables

List of Acronyms

A2P	Application to Person
AIT	Artificial Inflation of Traffic
CBS	Convergent Billing System
CDMA	Code Division Multiple Access
CDR	Call Detail Records
CFCA	Communications Fraud Control Association
CLI	Calling Line Identification
CRM	Customer Relation Management
ESME	External Short Message Entities
ESN	Electronic Serial Number
FASG	Fraud and Security Group
FMS	Fraud Management System
GSM	Global Stations for Mobile communications
GSMA	GSM Association
GT	Global Title
HLR	Home Location Register
HPMN	Home Public Mobile Network
HPMNO	HPMN Operator
HUR	High Usage Report
IMEI	International Mobile Equipment identity
IMR	International Mobile Roaming
IMSI	International Mobile Subscriber Identity
IPRN	International Premium Rate Number
IRSF	International Revenue Share Fraud
ITU	International Telecommunication Union
LTE	Long time Evolution
M2M	Machine to Machine
MAP	Message Application Part
MGF	Mobile Ecosystem Forum
MMS	Multimedia Service
MO	Message Originator

MSISDN	Mobile Station integrated Service Digital Network
MT	Message Terminator
MTP	Message Transfer Part
NGN	Next Generation Network
OTT	Over-The-Top
P2A	Person to Application
P2P	Person to Person
PRM	Partner Relationship Management
PSTN	Public Switched Telephone Network
SCP	Service Control Part
SIM	Subscriber Identity module
SIP	Session Initiation Protocol
SLR	Systematic Literature Review
SMPP	Short Message Point to Point
SMS	Short Message Service
SMSC	SMS Center
SMTL	Shor Message Transfer Layer
SS7	Signaling System Number Seven
SSP	Service Switching Point
TCG	Test Call Generation
VAS	Value Added Service
VLR	Visitor Location Register
VOIP	Voice over IP
VPMN	Visited Public Mobile Network
WCDMA	Wideband CDMA

1. Chapter One: Background of the Study

In less than forty years, mobile communications have surpassed the traditional fixed line telephony and become an integral part of everyday life [1]. Value added service (VAS) is one of rapidly growing mobile communication services since the first generation of mobile technology. Short Message Service (SMS) is the main service of VAS and provides a means for sending a message of a limited size (160 Characters) to and from subscribers' equipment and machines. It was standardized and implemented in Global System for Mobile communications (GSM) networks in 1992 but first developed in early 1980s [2].

Before SMS innovate station-to-station radio telegraph, telex (tele printer), teletext, and radio paging was used for market price announcement and one-way messaging. SMS is made up of **standards**, **protocols** and **infrastructure** that make text messaging the most popular data service on mobile networks [1]. The modern SMS ecosystem includes a wide variety of non-traditional carriers, External Short Message Entities (ESME's) gateways, resellers and Over The top (OTT) services.

The introduction of telecommunications in Ethiopia also dated back to 1894 [1]. The services provided by ethio telecom is growing from fixed telephone to fixed /wireless, Internet (dialup and broadband), mobile (pre-paid and post-paid), Code Division Multiple Access (CDMA) voice, internet and data, Wide (WCDMA) high speed internet and voice, 3G and recently 4G Long Term Evolution (LTE) and other VAS like SMS, MMS [3]. SMS service is introducing in ethio telecom by the Next Generation Network (NGN) project in 2004.

SMS report shows that number of SMS message transaction worldwide around 1.67 trillion messages were sent worldwide in the year 2017, with the volume set rise to 2.8 trillion in 2022 [4]. Some of the applications of SMS message are, User to User text messaging; Informational messaging or one way message that is time-sensitive; Notification services such as Premium base services; short news, sports, traffic, weather, stock market quotes movie times and more can be provided on request; and Mobile commerce [5]. The increasing use of in various areas and sensitivity of the content make SMS service vulnerable for different types of fraud.

1.1. SMS fraud

Different SMS frauds are existing since the beginning of the service. Different academic literatures and fraud management company documentation declare around nineteen different types of SMS frauds [6, 7, 8]. Some of them are SMS Bypass, SMS malware, SMS spam, and SMS Faking. Ethio telecom also one of the victims by such frauds.

To mitigate SMS frauds a variety of mitigation techniques are proposed by fraud management companies, industry forums, academic researchers and other responsible parties [7, 8]. Telecom operators implement these techniques, but the fraud is still a challenge for the industry [8, 9]. So that, it is important to study why the mitigation techniques are not effectively mitigate SMS fraud.

To understand and mitigate SMS fraud identifying modern text messaging ecosystem, fundamental technologies, and fraud root causes are important [9]. Untrusted relationship between regulatory bodies, existence of varieties of operators, unknown content providers, fake subscribers, unsatisfied employees and other external parties are the main causes keep SMS fraud as a challenge [8].

On other research works taxonomy-based fraud mitigation solutions are proposed. Security and different telecom frauds [9, 10] taxonomies are constructed these solutions give a holistic view for fraud root causes, vulnerabilities, exploitation techniques, and the way fraud benefit fraudsters [9]. Generally, taxonomy-based solution gives a comprehensive view to clearly understand the topic raised.

1.2. Statement of the Problem

Telecom fraud related researches approved that, legacy telecom network security leakage, interworking of new technologies, interconnect billing complexity, including lack of knowledge on fraud root causes and the situation where telecom industries keep telecom fraud secret, are among the reasons which made telecom fraud complex and unresolved issue [9].

Fraud is the main reason for telecom operator's revenue lose [11, 12]. CFCA 2017 survey estimated that a revenue of 29.2 Billion US dollar is lost due to telecom fraud out of 2.3 Trillion US dollar total revenue [12]. 2016 SMS fraud survey estimated 20 % of SMS traffics are

illegitimate [13]. SMS fraud not only affect the industry it also affects subscribers in different ways, such as personal information leakage, and bill shock (it is happening when SMS messages are sent to premium rate numbers without the user knowledge). To mitigate such frauds a variety of detection and prevention tools and techniques are applied but, SMS fraud is still a challenge for telecom operators [12].

1.3. Hypothesis

Developing taxonomy is a possible means to enhance existing SMS fraud mitigation practice, because it gives a comprehensive view of the fraud root causes to apply appropriate mitigation technique.

This research will analyze the below research questions:

- What are the different technologies used by of SMS?
- What are the different SMS frauds and mitigation techniques?
- How taxonomy-based approach improves SMS Fraud mitigation?

1.4. Objective

1.4.1. General objective

The main objective of this thesis is to improve current SMS fraud mitigation techniques implementation by developing SMS fraud taxonomy. The taxonomy is used to link between fraud scheme and its root causes to the corresponding mitigation techniques.

1.4.2. Specific objectives

Specific objective of this thesis includes:

- Conduct systematic literature review on the domain
- Identify the different tools, techniques, and standards that are applied to tackle SMS frauds
- Analyze and understand SMS fraud nature at ethio telecom

- Develop SMS frauds mitigation taxonomy to improve fraud mitigation techniques implementation.

1.5. Method

1.5.1. Taxonomy construction

To construct the proposed taxonomy; a taxonomy construction procedure is designed and followed. Theoretical and empirical analysis are the main part of the design, the sub sequent procedures are taxonomy refinement and evaluation phases. The theoretical analysis is studied under systematic literature review (SLR). For SLR a verity of researches, books, domain related publications, white papers from industry groups and proprietary documents are referred. Empirical analysis and evaluation are conducted based on ethio telecom SMS related data. For taxonomy construction cause and effect [8] and, question and answer [14, 15] methods are applied.

1.5.2. Used tools

The taxonomy is design using visual paradigm v15.0 mind map method and Microsoft Visio block diagrams. Other pictures on this thesis are also designed using the same tools. The evaluation also analyzed using oracle database with PLSQL and Microsoft excel.

1.5.3. Data collection and analysis

Empirical data are collected from ethio telecom different divisions through work around method, informal interview, discussion, Call Detail Records (CDR) and customer information related data from different information systems databases and soft switches.

1.5.4. Evaluation technique

The taxonomy evaluation is conducted by analyze the CDR data and implement to the specific fraud case based on the mitigation techniques proposed in the taxonomy. oracle data base with PLSQL and MS. Excel are used for data analysis.

1.6. Scope and limitation of the study

1.6.1. Scope of the study

The scope of this study is to propose SMS fraud mitigation taxonomy by studying the state of the art through systematic literature review combined with empirical analysis of ethio telecom SMS fraud mitigation practice. Finally improve SMS fraud mitigation implementation techniques.

1.6.2. Limitation of the study

As the aim of the study is not giving exhaustive list of SMS fraud ecosystems the taxonomy doesn't contain all components. There will be other points which are not include on the SMS fraud mitigation taxonomy.

1.7. Significance of the study

Telecommunication technologies and services are growing rapidly, similarly telecom fraud techniques are also changing accordingly. Telecom operators spend more time and money to detect and prevent fraud, but telecom fraud remain serious issue. Interconnecting emerged technology with existing networks make telecom fraud more complex. Telecom operator's loss 3% of their annual revenue because of telecom fraud [11, 12]. Loss of customer satisfaction is also additional failure for operators. To find out the root causes of such loses and the weak areas telecom companies spend a lot of money and time. The money and time spent to mitigate frauds are equivalent to the money they invest for new technologies [9].

The emergence of smartphones makes SMS a vital communication method for private, secured and fast communications, unfortunately SMS are vulnerable for different attacks. Such as SMS hacking, SMS Malware, SMS spam. It is one of the high impacted telecom frauds which affect both operators and subscribers [16, 14].

Ethio telecom and its subscribers also affected by different SMS frauds. Ethio telecom detect around forty-two million malware messages per month by using content filtering method. Which is around 1.2 million messages daily since 2015. These messages are blocked after affecting the subscribers and making ethio telecom system congest.

SMS spam also one of SMS fraud exist in ethio telecom, SMS spam is referred as unsolicited messages which is sent by the content provider to gain revenue through advertisement or by sending call me back messages to charging the subscriber in premium services charges. in August

2018 ethio telecom 49 fraudulent short messages service numbers are blocked because of SMS spam. The short numbers are detected based on customer complain, but these fraudulent service numbers are launched their services since 2016. These shows that SMS fraud mitigation methods using in ethio telecom are insufficient because, the fraud is detecting after affecting the subscribers and operator.

1.8. Organization of the thesis

The reset of the paper is organized as follow, **Chapter Two** contains literature review and related works. **Chapter Three** discuss the empirical analysis, **Chapter Four** discusses the taxonomy construction building blocks and finally propose SMS fraud mitigation taxonomy. **Chapter Five** is taxonomy evaluation based on empirical analysis and data collection from ethio telecom. **Chapter SIX** is all about the recommendation, future works and conclusions.

2. Chapter Two: Literature Review

On this chapter systematic literature review is conducted by locating published literatures found in diverse journals and industry documentations such as; Google Scholar, Springer Link, Science Direct, IEEE, eXplore, Wiley online library, including Industry specific documentations: such as ITU, i3 Forum, GSMA, TM Forum, SYNVERS, Arrex, and MEF fraud manuals.

This chapter has five main sections. The first is Key SMS **technologies** which describes three main technological areas Network and Protocol, Service and actors. The second section is technology **vulnerabilities**, third is SMS **fraud** and its classification. The forth section contains SMS fraud **mitigation** techniques. These four sections are discussed by categorize in to three sub technologies which are network/protocol, service and actor.

Network and protocol sub technology contains Key mobile and IP networks and its components including the protocol used to deliver SMS. The **Service** sub technology has different SMS service types (such as P2P, A2P and M2M) and service providers, content providers and third parties are discussed under service section. The **actor** sub technology consists of security solution (firewall, antivirus) and fraud management providers, mobile OS and application developers, content providers, consumers, and end users.

The fifth part of the literature review discuses related works, this related work part reviewed six literatures. All the papers are related to security and fraud taxonomies. Each related work strength, limitation and lesson learnt are also discussed.

2.1. Key SMS technologies

SMS is developed in the mid-1980s by GSM for second generation mobile networks [2, 1]. SMS evolved dramatically since its start. Short messages timely delivery, interoperability and ubiquity of the service keeps its popularity till today [1]. Early radio teleservices station-to station radio telegraphy and radio paging; one-way broadcasting allowed users to receive notifications services from nineteenth century are an early touchstone of transmitting a short message [2].

SMS is a store and forward way of transmitting messages to and from mobiles. The messages from the sending mobile is stored in a central SMS center which then forward it to the destination mobile

[1]. This means if the recipient is not available; the short message is stored and can be sent later. Each short message can be no longer than 160 characters, while these characters can be text (alphanumeric) or binary Non-Text Short messages [17] .

The fast growing of SMS technologies such as network architecture, protocols, service, standards, and emerging of smartphones govern new messaging services. Such as picture messaging or Multimedia Messaging Services (MMS) appear on the market in 2002. Premium SMS and MMS services, IP-based mobile messaging, and Stand-Alone OTT messaging services [2]. The three main SMS technologies network and protocol, service and actor are discussed in the below section.

2.1.1. Network and protocols

2.1.1.1. SMS network and components

The basic GSM network architecture is made up of three interconnected parts. The first is the mobile station subsystem, it contains two elements. The first component is the user's mobile handset or mobile station (MS). It contains a subscriber identity module (SIM) card that allows users to make calls or send data through a mobile network. The MS also has an international mobile station equipment identifier (IMEI) number, which is unique to the handset. A mobile handset also has a radio transceiver, the display to the user and a digital signal processor to send and receive calls and data [1].

When users send a text message from their phone, the handset transmits the message to the second part of the network architecture known as the base station subsystem (BSS). BSS is made up of a base station (BS) and a base station transceiver (BST). The BS and BST hands off the message to the network's closest Message Service Center (MSC), which is an intelligent terminal connected to other terminals. The MSCs and the data base (DB) that store the routing and teleservices makes up the third part of the network architecture. The SMSc which is connect to MSCs locates the receiver's handset through geolocation registers DB stored by the Network Provider and send off the message [1].

Figure 2.1:1 illustrated the traditional system architecture of the GSM network and the transmission of a text message that relies up on an SMSC as an intelligent terminal. When a mobile station sends a message; Mobile originating (MO) procedure is take place by sending the SMS to

the base station which is near to the user. Then the Mobile Switching Center (MSC) hands-off the data to the SMS center (SMSc). Which store messages and forward after checking on Home Location Register (HLR)/ Visitor Location Register (VLR) database for user and routing information. Finally deliver the text messages to users in mobile terminating part through the appropriate MSC

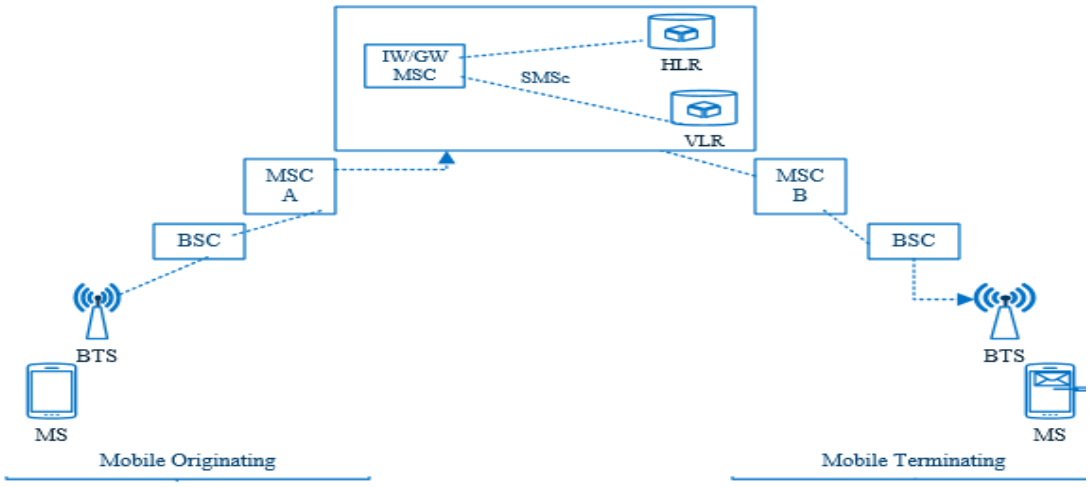


Figure 2.1:1 Traditional GSM network, MT and MO messages

Traditional telecom infrastructure has been deployed as monolithic entities each platform using different hardware and software, and different proprietary interfaces. SMS technology using for other generation of message transaction are similar.

Mobile Switching Center (MSC); The MSC is the equivalent of the local switch inside the mobile network. It provides very similar services to a switch but uses virtual circuits over radio channels instead of physical voice circuits. **Base Transceiver Station BTS;** delivers the message through wireless (Air interface), from BTS to MS. The MSC consist of Equipment Identity Register (EIR) and Authentication Center (AUC), which handles mobile authentication devices and validates that the messaging is originating from a valid device. MSC is connected to SMSC, where the messages are stored in the queue, and waits to get delivered to the respective user. The role of the MSC is to determine the location of the user to deliver the message by querying the VLR/HLR and sends the message to BSC. The BSC then delivers the message to the MS through BTS. When the user receives the message on his mobile phone it is usually stored on the device. The storing of the messages is performed by SIM card of the MS [1].

Home Location Register (HLR); HLR is a core database that keeps track of subscribers. It contains information on the current account status and provides authorization information for billing. When a call or SMS is trying to reach a subscriber, this is the node that is queried to find out where in the network that subscriber is [18]. **Visitor Location Register (VLR);** The VLR is the database attached to an MSC that keeps track of all the phones currently "registered" to it, informing other nodes of status changes, and checking authentication information registered [18].

Short Message Service Center (SMSC); The SMSC is the clearinghouse for SMS messages on an SS7 network and provides store and forward services. It is a network element in the mobile telephone network, in which SMS is stored until the destination device becomes available. Each mobile telephone network that supports SMS has one or more messaging centers to handle and manage the Short messages [18]

Modern SMS network architecture

The text messaging network includes a much wider range of participants and channels by which messages are delivered to phones. Whereas phone numbers once indicated a specific mobile device as an endpoint and were costly to acquire, text messages many now pass through a range of different domains that never touch a cellular network before being delivered to a mobile device, specific geographic area or even a single customer. As such, they violate many of the assumptions upon which the previously mentioned security services were founded.

Figure 2.1:2 shows the components of the modern SM ecosystem. External Shor Message Entities (ESMEs) are the main players in modern SM ecosystem. ESMEs form an entire industry dedicated to facilitating the sending and receiving of messages for large-scale organizations for purposes as diverse. They act as gatekeepers and interfaces to SMS. Some have direct connections to SMSCs in carrier networks while others resell such access purchased from other ESMEs [17].

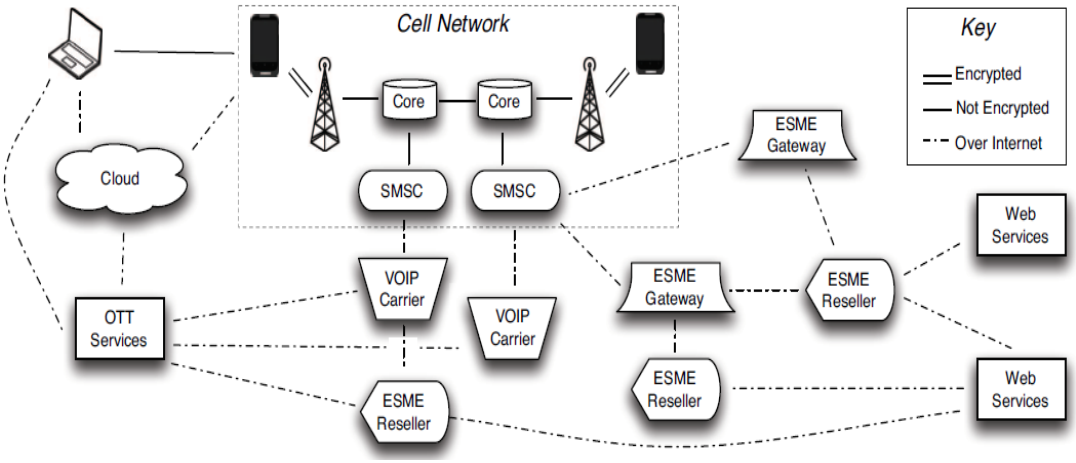


Figure 2.1:2 Modern SMS ecosystem [17]

2.1.1.2. SMS protocols

The structure of the SMS was developed as part of GSM, but now it is being carried out in the scope of 3GPP activities. The messages can be sent from mobile devices using the network (GSM/UMTS/LTE) and from ESME such as Internet hosts, telex etc. Messages can travel in both directions which communicates on the signaling links and allows messages to be received while the user is calling. Since the payload of a single message is limited; multiple text messages can be sent to the user, and the built-in software will accordingly concatenate it in most of the smart-phones [5].

SMS SS7 protocols

SMS messages are transmitted over the Common Channel SS7. Which is a set of telephony signaling protocols, used to set up and tear down most of the world's PSTN telephone calls. CC SS7 is a global standard that defines the procedure and protocols for exchanging information among network elements of wire line and wireless telephone carriers. These network elements use the SS7 standard to exchange control information for call setup, routing, mobility management, number translation, local number portability, prepaid billing, SMS and other mass market services etc. [19].

SS7 is built as layered architecture. Each layer plays a specific role the lowest three layers form the message transfer part (MTP) which is responsible for the secure and reliable routing of

messages, the content of which is provided by higher layers. MTP uses signaling links for routing messages to their destinations. Higher layers have different functionalities and are implemented as required by the network [19].

The standard protocol building blocks that support SMS and associated operations are **MTP1-3, SCCP, TCAP, and GSM-MAP or IS41-MAP.** All these software components must exist within the system. The specific operations supported within the MAP modules vary, depending on the node function, but these are simple for SMS operations. **Message Transfer Part (MTP1, MTP2, and MTP3);** MTP protocol layers reliably transport messages inside the SS7 network. MTP1 and MTP2 handle the physical link and link management. MTP3 handles routing, route management, and node availability up and down the protocol stack.

Signaling Connection Control Part (SCCP); SCCP provides connection service between two nodes within the SS7 network. It uses the MTP services to route messages between nodes. **Transaction Capabilities Application Part (TCAP);** TCAP is the protocol that uses the services of SCCP and provides a standard schema for transactions between nodes in the SS7 network. **Mobile Application Part (MAP);** The MAP layer uses the TCAP layer and provides the specific functions for the operation of the mobile network. Mobile-specific queries between nodes for routing and status use this protocol. The SMS service is defined in the core network by this protocol, and this is what provides the send/ receive capability to an SMS application.

MTP, SCCP, TCAP, and MAP provide services to each other and ultimately the applications that are the basis of operation for the SS7 network. Intel provides protocol "Stacks" such as the one described here to speed SMS deployment in SS7 networks.

SS7 architectures consists of three basic entities **Service Switching Point (SSP);** SSPs setup, manage and release voice circuit required to make a call. The main function of SSP is to use the information provided by the calling party and determine how to connect the call. SPP's uses a global title to determine how to connect a call using its routing table. **Signal Transfer Point (STP);** direct signaling units to the destination signaling points. If an originating SSP does not know the address of a destination SSP, the STP must provide it using Global Title Translation. **Service control Point (SCP);** SCPs provide database access needed for advanced services. STPs performs Global title translation using SCP.

SS7 over IP; IP based data transfer is fast growing in the telephony industry. SIGTRAN standards, describe a way of presenting SS7 signaling information over an IP transport in such a way that all the benefits of SS7 are maintained. SIGTRAN primarily is used at the interface between PSTN and IP networks. **Simple Control Transmission Protocol (SCTP);** has been defined that to ensure reliable transfer of information in a way that meets the requirements of SS7 systems [19].

The Short Message Transfer Layer (SMTL); SM-TL is used carry the messages that originate at the application layer with the delivery reports. The SM-TL of the MS and SMSC communicate with each other using SMS-TP. **SMS Submission Report;** when a user sends the message from his mobile phone, it is transmitted to the SMS Center. After reaching the message to SMSC, it will send back a message submission report to the sender's mobile phone to acknowledge of there were no error or failures. If no error or failure is detected, the SMSC will send back a positive submission report to the mobile phone else it sends a negative submission report [5].

SMS over MAP; it is working for message for 2G and 3G. Three MAP interfaces have been defined to support SMS; the first is HLR and SMSc the second one is interface between MSC and SMSC and the third is SGSN and SMSc. MAP interface is built on top of SS7 using TCAP, SCCP and MTP layers [3]. SMS over **Diameter;** diameter protocol was introduced with 4G to transport SMS between MME and SMSC, could also to apply SGSN supporting EPS interfaces [3].

In general, two basic technologies are used to route and deliver mobile messaging which are IP and SS7 protocols. While IP-based protocols such as Short Message Peer-to-Peer (SMPP) are used to exchange SMS messages between carriers [18, 2].

2.1.2. SMS services

SMS message service is an alternative to voice communication over the telephone when silent, private, or very brief communications are best [1]. ITU estimation report shows that number of SMS sent in the year 2010 are around 6.1 trillion and around 200,000 SMS messages are sent every second [22]. It is also the second revenue generating service for telecom service providers next to voice service.

The main types of SMS messaging are Person to Person (P2P), Application to Person (A2P) and Machine to Machin (M2M). Industry analysts estimate global A2P messaging traffic of the year

the year 2017 will rise to 2.2 trillion [24]. A2P messaging is omnidirectional SMS messages generated by a software application. The main categories of P2P, A2P and M2M SMS applications are User to User text messaging, Informational messaging or one-way message that is time-sensitive. Notification services, Premium base services: short news, sports, traffic, weather, stock market quotes movie times and more can be provided on request, and Mobile commerce.

Globally, many mobile network operators do not settle termination fees for internationally originated P2P messages. Because for every SMS sent can be expected a replay. It makes the two parties originated and terminated operators are equally advantageous. Also, operators eliminate the complexities of settlement. Some operators using this agreement for SMS Bypass by using for A2P Messaging.

Application to Person **(A2P);** A2P messaging is omnidirectional SMS messages generated by a software application. The main categories of P2P, A2P, P2A and M2M SMS applications are; **User to User text messaging; Informational messaging**: typically, one-way message that is time-sensitive. **Notification services**: it is sent to notify the users who have email, callback messages or voice mails, **Premium base services**: short news, sports, traffic, weather, stock market quotes movie times and more can be provided on request, and **Mobile commerce:** users can buy goods and services by using their mobile.

SMS popularity evolved new technological services; such as **Multimedia Messaging Service (MMS)** or picture messaging**, Premium SMS**; Premium SMS service charge users a premium to deliver additional content, such as ringtones or the ability to cast a vote on television programs. **IP Based Messaging;** IP-messaging use the open internet to deliver messages, without the requirement of passing through the carrier infrastructure [2].

2.1.3. SMS actors

As the mobile messaging market evolves, the benefits of new technology and the proven dependability of SMS switching technology are beginning to converge; as a result, each is adding value to a more open and flexible messaging ecosystem. Several companies from the mobile handset, telecom, internet, and software industries are participating in the mobile messaging value chain [2, 20].

Currently mobile network operators (MNO) and standardization bodies are the main actors on mobile SMS service. Social network players (Facebook, Myspace), OEM and platforms (apple, RIM), Carriers (OTT; VOIP), providers (WhatsApp, Skype), Aggregator clients, and SMS wholesalers are considered as third parties [2]. Security device consumers, smart phone Operating System (OS) and application developers. Aggregators and regulators are considered as actors.

2.2. Vulnerabilities

SMS service has led to a numerous of vulnerabilities, these vulnerabilities are existing in all technologies. Telecommunication networks and components consist of heterogeneous components executing specific operations that can be composed to implement complex aggregated services [21]. Weakness of existing network and protocol technologies are becoming a cause for different vulnerabilities. The ss7 protocol suite was standardized under the assumption that only the trusted parties (Government and Large companies) would be operating telecom networks [21, 19]. Lake of service provisioning and the increasing number of service providers, carriers and actors on the value chain make SMS service vulnerable [9].

2.2.1. Network and protocol vulnerabilities

SMS network vulnerabilities are many, some of them are **lack of mutual authentication** between MS and BTS. Because the authentication procedure is a one-way process, which means only BTS can authenticate the MS but not vice versa. The authentication process requires the IMSI or temporary mobile subscriber Identity (TMSI) if the device to authentication it [5].

The other vulnerability is **fallback to lower technologies**, it is happened when an MS attempts to connect to the appropriate network connection (UMTS or LTE) and is not successful to establish the connection, it eventually downgrades to connect the lower network. This limitation opens the door for fake BTS deployment and establishes a fake connection with the MS. By performing such fake connection, encryption for the data communication and all the network traffics are capture. This type of vulnerability is observed in UMTS network that also holds the GSM/GPRS/EDGE network capabilities and are configured to connect forcefully to GSM network whenever the appropriate network is not available [5].

SMSC vulnerability case is happed if an attacker gets access to SMSC, then there is the possibility to read or modify the messages in the queue or also read the SMS traffic passing through the system. The text message is neither encryption not integrity check mechanisms are enforced during its transmission across the GSMs. And its nature of operation to store-and-forward makes things even worse because of the number of locations where the SMS data is available to others in clear format. When it reaches at SMSC it is also stored in plain text format [18].

ESME uses SMPP protocol that depends on TCP/IP connection to connect the SMSCs. TCP/IP lacks security properties such as authenticity and privacy of the data passed over the network. In general, there is no security mechanism defined for SMPP and the data exchanged between two entities is in plaintext and may be intercepted over the Internet. Capturing and modifying the data during OTA transmission, Loss of SMS messages during transmission, SMS Spoofing at Authentication server, Lack of protection for message passing through SS7, IMSI catcher [18, 5]

SS7 vulnerabilities; IMSI catcher, since the IMSI can lead to other threats it is not transmitted over the air interface rather a randomized Temporary Mobile Subscriber Identity (TMSI) is used over the air. However, if an attacker can obtain the TMSI over the air interface and has access to the SS7 network, then the SS7 protocol can be used to ask what the IMSI is associated with the TMSI. An attacker can use the SS7 MAP and its normal procedure for delivering a text message to a subscriber to obtain the IMSI. **Intercepting a subscriber SMS messages;** the intruder will act like an MSC/VLR and sends and MAP-Update-Location (UL) request directly to the HLR subscribers. Once UL procedures are complete the subscriber will not be able to receive any message and the intruder spoofs the network into believing that they are now the new MSC [19]

2.2.2. SMS service vulnerabilities

One of the important challenges in the mobile communication industry is to ensure the mobile services are properly used and not open to abuse. SMS services and service providers are many. Service verity and a growth number of careers creates many weaknesses in the service. Such as by manipulating service agreements and international regulations principles sending abusive and free massages. There are many agents who take the service from telecom operators to provide the services. The mobile agents while roving in a network bring them the fear of viruses, Trojan horses, and another offensive threats [22].

2.2.3. SMS actors vulnerabilities

A verity of actors exists in SMS ecosystem, each actor has its own role on the advancement of SMS. Even though, a lot of leakages are coms from different actors intentionally and none intentionally [9].

2.2.3.1. Manufacturer and consumer related variabilities

Smart-phones provides various features than traditional phones such as Internet services, advanced multi-processing applications such as location services and powerful OS. The primary functions of OS are to control the security, performance and extra features of the smart phones. The rapid increase of smart-phone market makes the OSs supports a broad range of services and features but focusing on features in some cases neglect the security. Some smart phone OS and their security leakages are discussing below.

Android Mobile OS; the protection domain of the android OS applications is limited by default, but to grant more permission for other activities the user must provide it during the installation process. Many mobile attacks are performed on Android smart phones with fewer computation tricks. Before installation the user must accept the Terms and Conditions to proceed further with the installation procedure. This is the responsibility of the user to decide if the application is safe to install.

The threats from malicious android applications during the installation process are; the application tricks the user to give permissions to various systems resources including APIs, the malicious code is hidden behind the correct application permissions, and sometimes the application tricks the user to enter confidential data such as credit-card number.

Android malware is always on the rise once the application is installed, it is hard to differentiate between the legitimate and malicious version. It is important to identify the malicious version of an application during installation by observing the excessive permission requests. For instance, the legitimate application request only for network communication and hardware controls but the malicious application to access the messages, personal information storage including network and hardware controls.

Apple OS (iOS); which has C/C++/C# programming nature and vulnerable to traditional C programming language weakness and bugs. The applications on apple smart-phones must be download from apple app store. It is the most secure app store because apple developers perform security testing of the applications and it is released on App Store to download if no malicious activity detect. An application that is developed by a third party is tested thoroughly using sandboxing. Sand box method helps to protect the application to do not spread itself and to check that it does not access sensitive information on the device. Following all the guidelines and security checks provided by apple for its applications, it is not easy to launce malicious application in App Store. To protect all the data accessed by the applications Apple iOS provides SDK for all the third-party developers to provide highest level of security for their applications.

Windows Mobile OS; it has the same vulnerability as iOS and to mitigate these vulnerabilities. Windows Mobile allows its developers to write secure code by using libraries and to launch applications in the store it must be certified and authenticated by the Microsoft developers. Applications also uses certificates that grant permission to run with privileged permissions.

Cross Platform Smartphone vulnerabilities; these vulnerabilities are using the security limitation of PC/laptop and smartphone. The infected PC can pass the attack to the smartphones through USB, shared network connections, email and during data transfer. Smartphones also pass the malware through tethering and the attacker can compromise the confidential information of the user's easily [5].

2.3. Fraud

Fraud can be defined as a deliberate attempt to misuse the products, services or processes of others without having to make any or at least a part of the payments [23].Telecommunication fraud is also defined as the unauthorized use, tampering or manipulation of a mobile phone or service [24]. Currently there is no standard definition for 'telecommunication fraud' [23, 9]. But it essentially involves using deception to make a personal gain dishonestly for oneself and /or create a loss for another. Ethiopian criminal law, Telecom fraud offence proclamation No. 761/2012 define fraud as "fraud is the crime" [25].

Since the beginning of commercial telecommunications begins, the fraudsters have been causing financial damage to the companies who offered these services [26, 27]. Telecommunication fraud has certain characteristics that make it particularly attractive to fraudsters [28]. This has resulted in the increase of frauds in today's technological environment [27]. Telecommunications fraud became fundamental issue for telecom operators. Telecommunications worldwide Industry Experts surveyed and estimate annual global fraud losses to be in the range of 60-70 billion (USD) [29]. Fraud negatively impacts on the telephone company in four ways which are finance, market, customer relation and shareholders perception [30].

Factors leading to telecom fraud are many some of them are failure to understand the complexity of new technologies, dissatisfaction of employees, weakness in operation systems, irresponsible business models and criminal greed, money laundering, political and ideological factors, ineffective audit system and free financial gain [9, 23].

2.3.1. SMS fraud

To identify SMS frauds understanding of modern text messaging ecosystem, fundamental technologies, regulations and international agreements are important [8]. The modern SMS ecosystem includes a wide variety of non-traditional carriers, External Short Message Entities (ESMEs) gateways, resellers and OTT services [18]. In the modern SMS ecosystem. The main perpetrators and victims are operators, third parties, service providers, customer's employees and other external parties [20].

SMS is one of the victim services in telecommunication, because in SMS ecosystem there are verity of actors and service providers are evolved. The service verity and its characteristics make the fraud types many [31].

SMS Spam: Unsolicited messages transmitted over a variety of electronic communications Medias [32]. Spammer could be individual, commercial or operators [31]. **SMS Flooding;** is a kind of spam which sent to all the users attached to the operator's network [32]. Spam and Flooding SMS messages are caused for lose customer privacy and data lose [8, 33].

SMS Malware: Malicious software (Viruses, worms and Trojan horses designed to access data or use services in an unauthorized manner [8]. Installing infected software without mobile subscriber

knowledge to compromises subscriber data and send messages to premium rate numbers. Malicious hostile and intrusive application or software under the form of code and scripts [34]. To rob sensitive information; disrupt service; spy on service activities; gain access to sensitive information; change terminal configuration; promote calls or SMS to PRN without the user knowledge [8, 7]. **SMS Virus** it is closely related to SMS malware and phone crash type of attack. Phone crashing attack of performed when a malformed message is delivered to the user. In the same sense, the SMS message can have a virus attached in the form of a link to download an application or redirects to a webpage. It can also affect the mobile phones by corrupting the OS or creating bad sectors in the file system [20].

SMS Grey Routes: The message is operated in a way either by changing the global title in the Mobile Messaging Part (MAP) layer or avoid detection on another operators Firewall [8]. **SMS Access hacking**: occurs when a party tries to hijack the credentials of a legitimate third party. Uses technical skills and knowledge to break up or gain illegal access to network service platforms or user devices [35, 7]. **SMS bypass**: occurs at the point when wholesale revenues resulting from voice termination continue declining [36]; whereas the SMS termination revenues stay elevated. Another factor is the SS7 network is vulnerable to A2P fraud schemes [7]. **Artificial Inflation of Traffic (AIT):** causes when a party uses MO interconnect revenue share as a way of generating profit by sending messages to itself. (The cost of sending a message needs to be lower than the revenue share returns of an interconnect agreement [8].

GT Scanning; send SMS MO to GT address from one MO to find unsecured SMS-C **MAP Global Title Faking:** the effect of a person or company manipulating a message by change a MAP parameter and gain access on SS7 network to reach mobile operator SMSc [35]. **SCCP Global Title Faking**: the act of sending a message that doesn't belong to a sender which has been leased from a third party and where the SCCP and MAP are manipulated [35]. **SMSC compromise:** Configuring a mobile phone to use an SMS-C that do not screen or validate the A-Party. Gain access to the international SS7 network, manages to reach a mobile operator SMSC at Message Transfer Point (MTP) level and send messages around the world without paying for them [35]. **SMS Farms:** a method of using a bank of SIM cards for delivery of A2P commercial messages by bypassing an official Bulk SMS interworking agreement. (The payment is in local rate not international A2P rate).

Application to person (A2P) bypass; the main sources of A2P SMS bypass are Grey route, Compromised SMSc, SIM farm, using SMS HUB for A2P messaging without agreements, mobile originated (MO) spoofing [7].

SMS Phishing also known as Smishing. It is a technique used like Internet phishing emails. The attacker attempts to fool the mobile phone users by sending fake SMS messages with the help of social engineering practices [8]. **SMS Spoofing** is performed by replacing the originator's ID with an alphanumeric text. **SMS Fuzzing** is an automated or semi-automated process that involves transmitting invalid inputs to the targeted mobile phones to trigger security problems and unexpected behavior. The unexpected behavior is typically something like program crashes that is not expected under normal test conditions. It is used to inject fuzzed SMS messages to the mobile phones and monitor the application behavior under stress conditions. In fuzzing, the data included in the SMS packet is malformed which performs unacceptable situation to mobile phones.

Threats to SMS instant Messaging Applications; during the registration of different accounts such as google, Viber, Skype on smart phones for application there are various ways for an attacker to hack the account to capture the OTP through SMS messages are **account hijacking;** it is happed during OTP send from the server the attacker can hijack the user account by-passing a fake mobile number instead of the legitimate user. **ID Spoofing** occurred ones the account is hijacked the attacker can spoof the sender ID. The attacker can also send malicious messages by manipulating the message. This attack is performed after the registering the account during the regular send and received message transmission.

Enumeration; most of the mobile messaging applications once registered access the address book and location services of the user. It compares all the entries in the list with the server and retunes the list of users who are using the same application. By providing access to the address book the main problem is that the attacker gets access to the all number and send our phishing messages or carry out a DoS attack [5].

2.3.2. Fraud classification

As fraud is a constantly changing threat, it is essential that the classification model is revised periodically to ensure that fulfills its goals. It is important that a common classification model is

widely adopted to ensure comparability of statistic and benchmarks, but also to ensure that all relevant information is collected a common format for distribution and to maximize the benefits of information sharing [31].

Telecommunication fraud is classified differently, earlier classifications complies in two categories which are subscription fraud and superimposed fraud. [37, 30]. Recently telecommunication frauds are classified in wide-ranging categories. Based on behavior, data source, technology, service type, users or usage and many more. Fraud in telecommunications have been classified by the technical way they are committed and non-technical purpose just for financial gains. A further classification can be done by considering whether the network abuse is the result of administrative fraud, procurement fraud, or application fraud [27]. In some document's telecom fraud classify simply in four groups contractual fraud, hacking fraud, technical fraud and procedural fraud [27, 23].

There are a lot of trade associations and fraud management companies are working on telecommunication fraud, by collaborating with telecom equipment manufacturers, regulators and telecom service providers. In this limited resource it is difficult to describe about all fraud classification. There are many more respective organizations working in telecommunication fraud like CFCA, KPMG, SUbex, i3 Forum and many more. But it is impossible to write about all in this paper. In this paper Some of international associations which are GSM Association (GSMA), TM Forum, SYNVERS and MEF fraud classification methods are discussed [29, 38, 39].

GSM Association represent the interests of mobile operators since 1987 worldwide. Across more than 220 countries, the GSMA units nearly 800 of the world's mobile operators with more than 230 companies [40]. GSMA FASG (Fraud and Security Group) was established in December 2014 and the mission of the group is to drive the industry's management of fraud and security matters related to GSM technology, networks and services [40]. GSMA first version fraud manual produced in 1996. To list and categories the various types of frauds. The 2017 version of GSMA fraud manual classify telecom frauds under the broad categories of; Technical fraud, Subscription fraud, distribution fraud, business fraud and prepaid fraud [41].

Tele Management (TM) forum Telecommunication fraud classification guide is developed as a periodically growing resource to arm operators with fraud type information and offer them a best

practice for a common fraud cases classification model. And the guide is structured to support Fraud Operations activities associated with the TM Forum Business Frameworks model [39]. Classified telecommunication frauds as Enabler Technique and Fraud Type [42]. Fraud enabler is the method or technique of getting access to the goods or service and perpetrating the Fraud, A Fraud Enabler can be an illegal action by itself. It is possible to have one or a combination of a set of Fraud Enablers for a specific fraud type [42]. Fraud Enables can be classified in four sub groups Attack Type, Fraudster Type, Location and Environment. Under each sub group there are various types of fraud like Subscription Fraud, PBX hacking, Arbitrage, SMS-C abuse and other. Fraud Types also classified in six sub groups Location, Environment, Objective, technology, Service and Supplementary Service and under each sub group there are other categories [42].

SYNVERS established in 1987, and become global leader in mobile inter-operability, mobile communications and mobile expertise.**Invalid source specified.** SYNVERS classified fraud in five broad range of threats there are Domestic, Roaming, Prepaid, Data and Subscription and under each broad category there are vast number of fraud types are categorized [38]. Under Domestic threats there are around eighteen fraud types are listed and some of them are LTE fraud, SIM cloning, SIMBox fraud, IRSF/PRS. Under Roaming threats around twelve Fraud types are categorized and some of them are SIM Cloning, SMS fraud, Call selling, GPRS High usage and Subscription. Under Prepaid threat around eight fraud types are sub categorized some of them are Manual recharge fraud, high balance fraud, scratch card abuse and internal fraud. Also, under Data threat five types Data usage frauds are listed. In the last category Subscription Threat around seven fraud types are listed and some of them are Identity theft fraud, dealer fraud, and Handset subsidy loss.

Mobile Ecosystem Forum (MEF) also classify SMS A2P frauds in four categories Network, Market, Enterprise and Consumer. MEF categorize eleven types of A2P Messaging frauds in these four groups based on the fraud scheme and fraud techniques. MEF categorization intention is by whom the fraud is committed.

2.4. Mitigation techniques

Due to the constantly changing nature of fraud, it is vital to accurately characterize and measure fraudulent events to help understand how fraud is evolving and how effectively the Fraud Management process in taking it. It is important to understand the context in which fraud is committed to take the right corrective and preventive measures. Fraud identification and detection is an increasingly important, expensive and difficult task in today's technological environment and the most difficult aspect of fighting fraud is identifying it.

For this research the mitigation techniques are categorized as technical and none technical. The technical methods are mitigation technique which is use any tool or system. None technical methods are the one which related to agreement. Policy, procedure, standard and awareness. Also, the mitigation techniques are classified in three technological levels network and protocol, service and actor.

2.4.1. Network and protocol level mitigations

2.4.1.1. Network/Protocol technical mitigation tools and techniques

Firewall and Monitoring; Apply filters on suspicious traffic [8], Identifying official routes to establish a commercial agreement or to close them [8]. Firewalls and routers within mobile operator networks to detect messages coming in from unauthorized channels [8]. SS7 Firewall/routing check when SCCP or MAP addresses are manipulated [19]. Real time monitoring or at the international signaling gateway with appropriate monitoring tools [43]. Trigger alarms to indicate increased traffic flows over the network [6]. Monitor large number of messages being sent to one or more destinations [35].

Test Call Generation (TCG); TCG from known application to identify the sending SMSc [43]. Test traffic generated manually through direct interaction with an application [7]. Monitor capricious loads on the network due to bulk SMS [19]. Identify the actual and 'grey route' SMS while sending SMS from TCG SIMs using boundless international routes [27].

SS7 signaling surveillance systems; Monitoring SMSC Global Title, or A_MSISDN is wrong or is taken from a valid originator [35]. Secure a mobile operator's SMSC at the Message Transfer

Part (MTP) level, the signaling point code [8]. No alphanumeric support on networks [8]. Set SCCP (Signaling Connection Control Part) alarms or reports, with random checks as a minimum, to verify that the calling party Global Title and Service Centre addresses match, or partially match [35].

Detect suspicious/abnormal traffic from a GT, Log the usage of specific MAP messages, either using native logging capabilities of the core network elements or through logs provided by quality of service nodes deployed to monitor network quality [43].

SMSc Security; Enough security precautions to prevent the SMSC from being used as a relay [5]. Packets these nodes have generated to see whether any other, previously unknown, attacks are ongoing. This could be used to build a 'profile' of potential malicious nodes [5]. Installed firewalls and filters to try and prevent SPAM, but these are typically configured to detect static keywords and can in some cases even stop legitimate messages from being correctly delivered [8]. Establish and monitor limits per SMSC based on known traffic patterns to identify high usage [6].

Block the possibility exists that an attacker manages to inject SMS messages into the messaging network with a 'spoofed' originator IDs [36]. Authentication the mobile originated leg of the message transfer [14]. Integrate specific DNS security protection to prevent server hacking as an IP Security policy [12].

Filter web applications; now use text messaging to interact with their customers [44]. Spam and malicious content filtering [6]. Filter messages contains a URL that looks valid or is potentially misspelled [5]. Brand's Canonical Name (CNAME) record in their Domain Name System (DNS) record to determine the true sender of the message and anything suspicious can then be blocked [5].

Network restriction; Operator can make restriction on Pre-registration so that an originator cannot be used until it is registered and approved, and No-alpha originators allowed [5]. Monitor messages not sent by a real mobile but is generated from a specific system with a C7 application [24]. Network support for "dynamic" alpha-tag originators [5]. Secure back-to-back contractual provisioning from a mobile operator down to a brand or enterprise [5].

Evaluate illegal use of the HPLMN SMS-C by a third party [24]. Permit only long numbers until a customer proves that they are who they say they are [18]. To avoid vishing attacks, the call recipient needs to check whether the caller is a trusted entity [16]. establish or enhance the incident management capabilities to be able to respond to incidents in the core network domain [29].

Blacklists, Whitelists, Machine Learning approaches [19,20]; tracing back an incoming call to its corresponding SIP-ISUP interworking GW to identify whether the display name has been spoofed [16]. SMS MO with a manipulated A-MSISDN (real or wrong) is coming into the HPLMN network from a foreign VLR (real or wrong SCCP Address) [24]. Hot list of phishing URL sites and block access or provide customers with a warning message before providing access [12].

Content filtering to look for specific originators [5]. perform cross-layer checking on addressing information, the SCCP layer and the information available, GT(s) in the MAP layer belong to the same operator [26]. Monitor if the displayed number of an incoming call is modified [16].

Content Monitoring; Monitor if many messages containing unknown SSNs are received without corresponding send messages (indicates a possible scan of the attacked operator's network) [26]. Monitor If an operator detects a non-standard sequence/order of packets in a certain time from a specific node, a new global title is generating traffic within its network and unusual sequence of aborts being generated or errors being sent to a global title different to what would normally be expected [26]. Detect a possible vishing attack through checking the verification of the display name of an incoming message during runtime [16]

Identify the possibility to send SMS message from the internet with the correct headers, without the recipient being able to detect that it comes from the internet [25]. Monitor intent delivery of new SMS received/ sent can't be easily intercepted or manipulated [10]. GTs monitoring approach allows operators to identify potentially compromised nodes from partners and to differentiate the traffic from the compromised 'black' nodes within the remaining range of 'white' nodes [26].

2.4.1.2. Network/Protocol none technical mitigation methods

Do not allows aggregators and application service providers (ASP) to blend direct connections with Grey Routes [5]. Educate closure of routes can result in the sudden failure of all messages

[5]. Protect Data sovereignty and privacy issues [6]. Plan to respond to newly identified bypass threats through refinement of their security policies [2]. SS7 SMS Inspection [23].

Evaluate discrepancies between protocol layers [23]. Security policies at the SS7 level [6]. Create clear guidance of what is and is not permitted in terms of message manipulation to remove any risk of ambiguity [5]. Ensure firewalls are correctly configured where reports or alarms can be created to detect whether a Service Centre address has been manipulated [5].

Do not provide the full Global Title when selling SRI's. A country code fulfils most legitimate use cases and if more of the Global Title is to be provided, the mobile operator should only do this for identified use cases [5]. Report to the Home PLMN of the originating MSISDN to have service removed [14].

Communicate if an operator detects that an internal or external global title is now acting strangely or inconsistently when compared to its past behavior, this could be an indication that the node associated with the GT has been compromised [26]. Ensure **proper configuration of a firewall** (compare the received Service Centre address and calling party Global Title in the Forward Short Message (FSM) instruction) [5]. Establish a continuous process for assessing and remediating any discovered vulnerability [29].

Educate customer, the incoming number (that is, caller ID) displayed on the phone screen is not enough to detect vishing attacks since vishers can modify the displayed number on the phone by using a technique called "caller ID spoofing" [16]. A combination of identifying legitimate originators and active monitoring of messaging traffic [5]. Implement concrete contractual back-to-back arrangement with the sending party and the value chain [5]. Knowledge base: how trick the SMSC by modifying the low-level signaling parameters of the MO message, and due to the assumption of trust in SS7[14].

2.4.2. Service level mitigations

There are also different kind of SMS service level mitigation tools and techniques. The main ones are deploying Fraud Management System (FMS), antispam system, implement data mining tools. Service provisioning (Price, Incident, market, consumer, subscriber), Policy (Reporting, Law enforcement Educational resources (Consumer, SP, CP, end user)

2.4.2.1. Service technical mitigation techniques

Establish a joined-up digital communications strategy within enterprises [16]. Protection on Global Titles and point codes from certain regulators [5]. Monitoring for breaches and taking enforcement action as necessary [6]. Passive detection through call detail record (CDR) analysis [6]. Increase controls and checks on who is bulk buying SIM cards via retail channels [5].

Counting Bloom Filters combined with **blacklist and whitelist** to detect SMS grey traffic on the fly and to block them [45]. Identify unauthorized access of SMPP gateway or SMSc [2]. Deploy counting bloom filter which is a variant of the standard bloom filter to keep track of the occurrence of blocks from a text message [21]. Establish end-to-end process to unambiguously identify the fraudulent parties [5].

Use **SMS Hub** to deliver traffics [6]. Establish a globally agreed process involving forensic investigators, where the co-operation of all parties is required. An independent company would be required to lead any investigation to ensure impartiality [5]. Set SMS Hubs to look for specific types of message manipulation [7]. Implement systems that ensure the SRI request and the subsequent FSM [5]. request is sent from the same Global Title [5]. Monitor high or unusual patterns of usage of SMS messaging or data usage per customer using the fraud management system [12].

Crowd-source information from actual users where possible [5]. Cross-mobile operator method of reporting [5]. Create and share a global blacklist of companies [5]. Provide industry-wide resources for monitoring, recording and mitigating Malware [5]. Static, dynamic and hybrid approaches by intrusion detection system. Static approach detects malware before the execution of program under inspection whereas dynamic approach detects malware after or during the execution of the program under inspection. Hybrid approach is the combination of static and dynamic approach [4.].

Dynamic analysis involves execution of application in isolated environment to track its execution behavior [27]. Implement cross-border registration schemes for alpha-tag originators [5].

Machine learning algorithms such as SVM or naïve Bayesian method for learning of known malwares and predicting unknown malware [20, 27]. a combination of identifying legitimate originators and active monitoring of messaging traffic [5]. Pattern detection [5].

Enterprises should advertise their short codes on their web sites, together with information detailing what a consumer should or should not expect to be asked by a bank or retailer [5]. Monitor Customer complaints [2]. Monitoring both patterns and message volumes [5]. Effective data management [5]. Create a central registration of enterprise and brand names and all associated short codes and originators [5].

Register enterprise and brand names and associated short codes and originators (local or global database) [5]. Anti-virus [12]. Develop and update a black list of blocked senders [12]. Deploy SPAM filters to identify repetitive content and volume [12]. Keep an updated white list of all allowable SMSCs [12]. Monitor latest phishing technique developments and variations on anti-phishing websites [12].

A database of SMS Originator Spoofs and SPAM that aggregators can access both nationally and Internationally [5]. Evaluate unauthorized routes causes confusing and volatile market prices [5]. Dedicated SMS fraud management system can be used to automatically generate test calls for tracing [2]. Detected by comparing the rate or number of messages in a selected message flow to a pre-selected defined average or expected load [14].

2.4.2.2. Service none technical mitigation methods

Proper AA19 / AA60 agreement [5]. Control market Price-led procurement activities carried out by aggregators and some Over the Top [5]. Protect the ability to meet an enterprise's SLAs can be affected [5]. Raise enterprise awareness of the causes and risks of Grey Routes [5]. Promote a consistent mobile operator approach to monitoring and filtering [5].

Close and migrate bilateral 'sender keeps all' routes to SMS Hubs in order to monetize traffic without impacting P2P message streams [5]. Educate aggregators to do not manipulate messages to be competitive [5]. Check if aggregator not receive a true Delivery Receipt (DLR)[5]. Report any suspicions to the targeted mobile operators as quickly as possible [5].

SMS inter-working agreement with the network whose SMSC is faked then once again there could be inter-operator accounting issues [24]. Educate enterprises to stress the relationship between cheaper messaging and poor delivery quality, lack of delivery receipts Increase the price of a message so that the price of an A2P SMS is sufficiently high to avoid mass, non-targeted SPAM campaigns [5].

Contracts Follow with third party suppliers [7]. Tell the ecosystem about these recycled numbers and the ecosystem is obliged to remove these numbers from any opt-in marketing databases [5]. Anti-spam policy that prohibits the use of the mobile network for initiating or sending mobile spam [7]. Potential penalties for breaching the anti-spam commitments, including possible suspension and/or termination of contracts [7].

Work co-operatively with other mobile operators to address spam issues [7]. Monitor fake player who made money by sending messages to premium line numbers [45]. Register enterprise and brand names and associated short codes and originators [5]. Ensure that where free credit is given, bots cannot automate the creation of accounts [5]

Implement a Code of Conduct for A2P platform providers and aggregators [5]. Suspicious Messaging processes, asking for Fake contract renewal [5]. Credit scores and personal financial status is at risk of damage [5]. Effective regulation of A2P vendors [5].

Inform users about social engineering practice to imitate legitimate companies in unsolicited e-mails, fake websites or social networking sites to entice people to share personal identity data and financial account credentials [12]. If the billing is made from the SMS-C data, the real subscriber will be invoiced. If the Billing is made from the TAP file, no one will be invoiced [24].

Log on criminal offence in most jurisdictions [12]. Facilitate joint enterprise, mobile operator and government initiatives to raise awareness [5]. Monitor frontline queries: customer questions and complaints [12]. Law enforcement must be involved for serious issues [5].

A2P SMS traffic so that commercial relationships can be established in advance [6]. Legal disputes [12]. Share knowledge of fraud cases within the global ecosystem [5]. Educate enterprises to highlight the true nature of the low cost of messaging [5]. Collect complaints about texts received by the customer from people they don’t know [12]

Review customer contracts, Terms & Conditions and/or Acceptable Use Policies, to ensure that up-to-date and relevant anti-spam conditions are included [7]. Appropriate customer consent and effective customer control with respect to mobile operators' own marketing communications [7].

2.4.3. Actor level mitigations

There are a lot of mitigation techniques implemented at actor level some of them are listed in technical and none technical section below.

2.4.3.1. Actor technical mitigations

The mobile subscriber must have a pricing plan with a low charge to send messages for this fraud to be effective [5]. Permission based analysis: Users have right to allow or deny the installation of applications [27]. Re-configure phone settings, applications or data [5]. Monitor Software's which that acts silently in the background, compromising sensitive data or exploiting the connectivity of the device [5]. Monitoring tools within aggregator and mobile operator systems [5].

Crowd sourced malware profiling system. The end user can consult this list to decide if he is installing a malicious application or not [46, 47]. A URL points to a website hosted by the rogue third party [5]. good practice to avoid phishing is to use bookmarks for your frequently visited websites [20]. Claim to be form a bank asking users to dial a phone number regarding problems with that bank accounts [48].

Monitor an attempt to illegally gather personal and financial information by sending a message that appears to be from a well-known and trusted company [20]. Collaboration with mobile operators to limit the ability of messages containing unauthorized or unregistered originators being delivered [5]. Install and use genuine applications provided by trusted vendors [20]. Anti-phishing tool from trusted vendors [20]. Block messages which use unregistered or unauthorized originators [5]. An increased reliance on mobile applications [5].

Bookmarking for known URL [5]. Enterprises should initiate communication with any affected consumer which explains the next steps, follow up and actions including number harvesting [5]. Forwarding the suspected message to a short code [8]. Secure a mobile device by a password and

other access control methods [20]. Subscribers can filter spam messages at their device depending on the type of device being used [12].

URL detection, enterprise not effectively managing a relationship with a consumer (education, inadequate data management) [5]. host-based and cloud-based protection, the technique that runs in mobile phone is termed as host-based technique. However, to improve the efficiency, the intense computation is offloaded to a separate server; this technique is called cloud-based technique [18].

Automatic end-to-end way to validate whether an originator belongs to a brand or not [5]. Identify the identity: sending abusive messages to an individual but pretending to be someone else [5].

2.4.3.2. Actors none technical mitigations

Educate mobile subscriber do not agrees to become a "mini SIM Farm" [49, 8]. Educate mobile subscriber to do not downloads and installs an app provided by a rogue third party [5]. Educate the user's about security and privacy and consequently the operator's reputation [2]. Working with governments and regulators to support industry [49].

Provide customers with information and resources [7]. Brands and enterprises may sometimes fail to properly manage consumer data correctly [5].

Educate the authenticity of permission requested by the application. Also, the safety of install applications from third party app stores [10]. SMS messages are used to collect money by sending messages to premium-rate numbers without user consent [13]. Smartphone users should implement a good anti-malware framework, only download apps from trusted app market [17].

SMS malware is software on mobile network accessing devices that causes undesired or damaging activities on the mobile device or network without the user's informed consent [14]. In general, it refers to software which runs on handsets without the user's knowledge, and which adversely affect the user and/or network [14].

Educate different forms of malwares, including deliberately or accidentally designed software running on the mobile handset which can generate excessive traffic, mobile viruses designed to transfer credit, perform DoS or some other type of unwanted effects, spyware designed to report on mobile activity, and so on [51]. Application Developers: policies governing secure coding and

privacy and do not access unnecessary information. Also, can use a unique identifier instead of the IMEI to protect [17].

App Market Administrators: strictly vet every uploaded app, and remove suspicious apps, Kernel [17]. A lack of awareness, among both consumers and enterprises, of potential risks [49]. Enterprises should communicate 'personal' information in messages such as a forename, secret word or phrase which the consumer has shared with them in advance [5].

Sites intended to assist with this fraudulent practice, Lead generation, by pretending to be a known company [5]. Educate users how to entice people to share personal identity data and financial account credentials such as online banking passwords and credit-card numbers [12]. Educate users to do not reply for spoofed website, or Faking messages ask for calling a premium phone number [28].

Protect sensitive personal and confidential financial information [5]. Educate: Intended to trick the victim into entering personal information for breaching the victim's account [30]. Educate consumers: Never give out your personal information in response to an incoming call or rely upon the Caller ID as the sole means of identification, particularly if the caller asks you to carry out an action which might have financial consequences [53].

Never reply to any suspicious SMSs [20]. hacking to gain access to a mobile subscriber's operating system and access information about accounts or data such as credit card, banking information or passwords for malicious reasons [5]. During application installation, permission can be accepted or rejected by the user thus delegating the permission management to the user [18].

Users carelessness; not sensitive to the fact that their smartphones are essentially are vulnerable to cyber-attacks [22]. Malicious applications send SMS to premium-rate numbers without user's consent [22]. Sending SMS at consistent intervals to such numbers, it can cause significant amounts of financial loss to the victim [13]. Malicious app. secretly gathers user's personal details and information and selling these details to marketers. DroidLight in Android, Privacy-A in iOS and SPIsSaga in Symbian [4].

2.5. Related works

Taxonomy is known to provide a systematic classification of elements in a domain and can be efficiently used to express concepts in a structural manner [14]. The term "taxonomy" refers to an order or classification of things according to specific condition. The reviewed taxonomy related literatures for this study are follow two types of taxonomy construction approaches. The two methods are question-and-answer [14, 15, 50] and cause-and-effect method [9, 46] and mind map representation is also used for the taxonomy graphical design [14, 51].

Four related works are reviewed and followed as a reference for these thesis work. The first related work is "A Taxonomy Study of XSS Vulnerabilities" published in 2017. The main objective of the work is to make a survey on detection/prevention of Cross Site Scripting (XSS) vulnerability. Then classify XSS on location (Clint, Server Hybrid), Detection type (Vulnerability, Attack, Hybrid), and detection techniques. Based on the classification method new Cross Site Scripting taxonomy is Propose. The taxonomy is used to analysis the mitigation techniques based on the classification. which are Clint side, Server Side or Hybrid based mitigation is proposed [52].

The second related work is "Defending against Phishing Attacks: Taxonomy of Methods Issues and Future Directions" published on 2018. To provide Taxonomy of various types of phishing attacks the researcher try to understand the background history of Phishing attacks, attack incidents and statistic reports. The classification is based on phishing mitigation techniques which are link based, website based, and header based. Defense mechanism taxonomy is proposed which contains a comparison of existing phishing website solutions [53].

The third related work is "New Comprehensive Taxonomies on Mobile Security and Malware Analysis" published in 2017. The aim of this literature is to provide a comprehensive Mobile security taxonomy. They reviewed mobile security literatures which are published from 1993 to 2015. On their taxonomy they developed a new leveling scheme for enumerating taxonomy contents. The highest level of their taxonomy hierarchy classifies the problem in android security, techniques used to solve the problem and evaluation. The resulting taxonomy hierarchy consists of 21 dimensions. Two types of classes namely conceptual and core classes and two separate sub taxonomies which are malware analysis and machine learning sub taxonomies [14]. Their new

comprehensive mobile security taxonomy and mobile malware analysis sub taxonomy having over 1,300 nodes (14 classes, 177 subclasses,528 elements, 382 sub elements, 72 attributes, and 149 sub attributes). The previous works they referred has a maximum of 25 nodes. The taxonomy is constructed through question- and-answer method [14].

The fourth related work and which is used as a reference for this thesis work is "Sok: Fraud in telephony networks" published on 2017. The research first tries to understand telephony ecosystem then build a taxonomy as cause-and-effect structure with five layers. The first layer is Root cause in this level the main causes of fraud enablers are settled. The main enablers on telephony ecosystem are legacy protocols, variety of technologies and services. The second layer is Weakness the weaknesses are the result of the root causes which are used to manipulate the service. The third layer is techniques used to manipulate the service. This leads the fraudsters to apply the fraud and get benefits from this. This is telecom fraud taxonomy and it helps to understand telecom fraud easily. From this taxonomy work the methodology, and the main nodes structures are adopted for this research [9]. In this taxonomy fraud mitigation is not included.

In addition to the above four literatures, other taxonomy-based works are also reviewed. Network challenges taxonomy is one of related taxonomy which constructed as; Fault➔Error➔Failure and using cause and effected method. Challenges are referred as network weaknesses or attacks, these attacks have been a cause for to develop faulty and vulnerable network, this vulnerability creates system error then it causes for failure [51]. The other taxonomy which used a cause and effected method is embedded system security attack taxonomy [50]. Security assessment of android software taxonomy also use a question-and-answer method. The first part of the taxonomy approaches positioning, which characterize the WHAT aspects. The second group of the taxonomy dimensions is concerned with classifying the HOW aspects [46].

The above related literatures are very supportive to understand how Taxonomy is used in IT, engineering and in telecommunication. Taxonomy construction methodologies are adopted for this research. The taxonomy construction methods used in the references are different but, the taxonomies make their domain easily understandable. In recent years many security and fraud related taxonomies are proposed, it implies that taxonomy is an important tool to clarify such complex areas.

3. Chapter Three: Empirical Analysis

This chapter contains the empirical study based on ethio telecom SMS fraud related data. The first part of the chapter is discussing about ethio telecom SMS fraud mitigation practices. The subsequent section contains data collection and understanding. The third section discuss data analysis and pattern extraction. The last part is chapter conclusion.

3.1. SMS fraud mitigation practices in ethio telecom

Ethio telecom prevent SMS fraud via **Anti-Spam system** keyword filtering method. **Blacklisting** international fraud numbers at the international gateways. Four SMS frauds are planned to detect using ethio telecom **FMS** which are Open SMSc, call back SMS, SMS malware, and SMS phishing, but it is not practical till the researcher finalize this thesis work. The reason is the data source is not configured to input the FMS.

One of SMS protection method which is using in ethio telecom is HUB agreements; ethio telecom is signed with two HUB operators BICS and Syniverse**.** The pilot HUB service is started in May 2018 with BICS. It is known that, it is not successful as expected because ethio telecom doesn't have firewall at gateways (SS7/SMSc) to filter bypass messages, which are not passes through HUB [43, 54].

Proper Interconnect and Roaming agreements; the main gates for SMS bypass and GT faking types of SMS frauds are violet interconnect or roaming agreements. Proper agreement and follow up is the main method to mitigate such frauds. Ethio telecom sign roaming agreements with more than 500 operators. Since 2015 ethio telecom signed an agreement with SYNVERS work as a data clearing house agent. Data clearing house agents are working with telecom operators to collect International Roaming CDR data from all roaming partners and settle the interconnect fee, sending high usage reports, and fraud suspect numbers for the telecom operators [6].

Network monitoring (revenue assurance tools); The other protection method is suspect numbers by monitoring the message transaction. The monitoring tool shows ongoing SMS and Call traffics. If any unusual traffic detects, the suspected numbers are extracted and send for further analysis [12, 40].

Bill complain; is also another means to detect SMS fraud. Subscribers are complaining when the payable bill is higher than they expected. The complains are further investigated by the fraud expertise then take appropriate action based on the investigation result.

Customer service log; Customer service log is also used as fraud mitigation tool. Subscribers are making calls to CS hotline number 994 for different reasons. One of the reasons is complain, fraud related complains are sent for further analysis. Based on the analysis result if any suspicious behaviors are detected appropriate action is take place.

3.2. Data sources

The data for empirical analysis is collected from ethio telecom different divisions i.e. Network, Information system, and marketing. Two type of data are collected document based and Call Detail Records (CDR) based. To understand the data discussion with domain expertise, work-around are conducted.

Document related data are policies, FMS fraud manual. Local and interconnect agreements documents; HUB agreement with BICS, roaming agreement documentation with Syniverse. Processes and procedures including fraud and other SMS fraud reports.

The CDR data are extracted from live systems such as Customer Relation Management (CRM), Partner Relation Management (PRM), Convergent Billing System (CBS), Mediation system, ethio telecom MSC soft switch, Short Message Service center (SMSc), and Antispam system.

3.2.1. CDR Data type and fields explanation

CDR data attributes are selected through the importance of the fields and with discussions with antifraud experts. All CDR data are collected from live systems and the data values are clean and have no unexpected or null values found. The useful attributes with explanations are shown in Tables 1 to 7.

Roaming CDR the selected attributes are International Mobile Subscriber Identity (IMSI) number, CDR type which differentiate between SMSMO (originator /sender) vs SMSMT (Receiver), Mobile Subscriber Integrated Services Digital Network (MSISDN), Number which the unique subscriber number received when the service is allowed. Home manager which is roaming partner,

OTHERTELNUM or receiver's number, start time, Mobile Switching Center ID (MSCID), and Deal Time which the SMS originate time.

Table 1Type of roaming CDR extracted from database

Roaming CDR	
Data field	Explanation
IMSI	Mobile apparatus unique number
CDR_TYPE	Differentiate the owner who originate the message
MSISDN	Unique Subscriber number
HOMEMANAGER	Roaming partner or service provider
OTHERTELNUM	Message receiver (MT) mobile number
STARTTIME	The message originate time
MSCID	Mobile Switching Center ID (which is unique for each MSC)
DEALTIME	Same as start time but sometimes varying if network issues

Interconnect CDR attributes are calling or senders number, called or receivers number, called and calling country, start time, IMSI and MSCID. Local CDR attributes are also calling and called number start-time, fee it is selected to know if the fee is deducted or not. If it is deducted it means the message is considered as fraud message and protected by antispam system. Other fields of CDR attributes are related to county and carrier.

Table 2 Type of interconnect CDR extracted from database

Interconnect CDR	
Data field	Explanation
ORIG_CALLING_NUM	Caller number who initiate the SMS
ORIG_CALLED_NUM	SMS Receiver number
CALLING_COUNTRY	SMS initiator country
CALLED_COUNTRY	The receiver country
START_TIME	The call start time
IMSI	Mobile apparatus unique ID number
MSC_ID	Mobile Switching Center ID

Local numbers CDR fields are Calling and called number which is subscriber numbers who send and receive the SMS. The SMS sent time, SMS fee per message, SMS receiver country and operator and, sender operator.

Table 3 Type of local CDR extracted from database

Local numbers CDR	
Data field	Explanation
CALLING_NBR	Senders subscriber number
CALLED_NBR	Receiver's subscriber number
START_TIME	SMS send time
CALL_FEE	Fee per SMS
CALLED_COUNTRY	SMS receiver's country
CALLING_CARRIER	Senders operator name
CALLED_CARRIER	Receiver's operator name

SMS CDR attributes are sender and receiver's numbers, SMS submit time which is the time submitted to the center, SMS status if it is successfully delivered or failed, timeout (Timeout is occur when the receiver mobile is switched off for a specific time of periods like three days), and SMS content the content is extracted in plain text.

Table 4 Type of SMS data extracted from SMSC database

SMS CDR	
Data Field	Explanation
CALLER	SMS sender subscriber number
CALLEE	SMS recovers subscriber number
SUBMIT_TIME	SMS submitted time at the center (SMSC)
SMS_STATUS	SMS delivered or failed status
SMS_CONTENT	The message content

High risk numbers are reported by GSMA and CFCA in monthly bases. The numbers are international destination numbers which are considered as high risk IRSF numbers. The high-risk number report has many attributes including the reporting country call times and other. For this research IRSF suspicious service numbers, their number range, number originator country and inserted date are extracted for this research.

Antispam report format is predesigned to extract as it is. The attribute fields contain Caller and called numbers as sender and receiver mobile number, prevent time; the message blocked time, and prevent keyword; the key word which is used to filter the SMS content.

Table 5 Type of IRSF data extracted from GSMA

IRSF high risk numbers	
Data field	Explanation
SERVICE_NO	Suspected service number
NO_RANGE	Range of the IRSF service number
COUNTRY	IRSF suspected number country
INSERTED_DAY	Number suspected date

Table 6 Types of Antispam report data extracted

Antispam report	
Data field	Explanation
CALLER	Sender's number
CALLEE	Receiver's number
PREVENT_TIME	Message blocked time
KEYWORD	Content filtering keyword

Ethio telecom block international SMS fraud suspected numbers at the gateway switches. The black listed numbers have two attribute fields which are blocked number in range and as a single number, and backlisting description such as a sender, as receiver or both are blocklist.

Table 7 Type of international blacklisted numbers extracted

International blacklisted numbers	
Data filed	Explanation
BLOCKED_NO	Blacklisted number in range or single number
SERVICE_ ATTRIBUTE	The action taken (blacklisted as Originator, receiver or both)

3.2.2. Data collection and understanding

3.2.2.1. Data collection

June and July 2018 SMS fraud numbers, which includes antispam protected numbers, suspected SMS numbers through network tool, RA tool and CS reports, Bill complains. The other data which collected are backlisted numbers at ethio telecom gateways and soft switches. International suspected high risk IRSF number ranges [40].

a) **ethio telecom Antispam system;** Around six keywords are configured for fraud message filtering, based on these key words the system prevents in average one point two million SMS malware messages per day. Around 66 million SMS in two months.

b) **Bill complain;** eighteen SMS suspicious numbers are considered as a fraud numbers from 27 bill complains in June and July 2018. These numbers CDR is collected from CRM and PRM for further analysis, and it is 20K records.

c) **Network/RA tool, CS report and manual analysis;** 23 international SMS fraud numbers are suspected in these two months. These numbers are added to blacklist at ethio telecom international gateway.

d) **IRSF** 10K international high-risk numbers are communicate as IRSF numbers by GSMA on September 2018. These numbers are communicated to all operators who join the forums. If the operator received these numbers require to act by blocking the numbers in its network.

e) **Blacklisted numbers;** From ethio telecom soft switches 1.6 million blacklisted numbers are collected for analysis.

f) **Roaming and interconnect CDR;** From PRM database suspected numbers 22K roaming and 2K interconnect CDR are collected.

g) **Local numbers CDR;** from CRM and CBS data basses suspected SMS fraud numbers 41k SMS CDR are collected.

3.3. Data analysis and pattern detection

3.3.1. Data analysis

Through data analysis different behaviors are extracted from the collected data some of them are as follow.

a) In the international SMS's the following behaviors are extracted
   - Short numbers and Alphanumeric are found as a sender number, but international short numbers should not allow in the receiver's operators network to protect itself from IRSF.
   - Unbalanced international transactions which are send and received various messages (Some of the numbers are received one million SMS per day).

b) Antispam system data; the antispam filter short messages based on the preconfigured key words. The pattern in the report; shows that from the average of 1.2 million daily filtered short messages. One million SMS are sent to one destination number which filtered by one keyword.

These messages are application registration request (REG-REQ) originated from customer mobile application, to the number 4478XXX.

c) Roaming CDR contain 22 thousand records; 50% of the records are none suspected pattern, but the other 50% of the records are suspected. The message is sent to short numbers; sent message to known international PRS numbers, and unbalanced SMS transaction also detected, and for some numbers 70% messages are sent to other country than their home country because the SMSc number found in the CDR is different.

d) Interconnect CDR only 1000 records are selected for further analysis the reset of the records patterns is not fraud. It is also observed that there are other messages are successfully sent to the same destination. This implies that the antispam keyword policy protects the message with specific keyword, but message is sent to the same number with other SMS content. It shows that the keywords are not enough to protect all the messages. So that it is better using blacklist and white list option of the antispam system.

e) Ethio telecom gateway blacklisted numbers are 1,600,000 million, from these numbers 1,300,000 are one country GT.

f) High-risk IRSF numbers are communicated but ethio telecom doesn't act to block these numbers. Ten of these known high-risk international fraud numbers are found in bill complains so that ethio telecom required to blacklist these numbers in its international gateways.

Table 8 Data analysis results

CDR Source	Total records	Pattern	Protection required
Antispam System	1,600,000	1Million to one B-number (app)	Black listing
		6910 to ethio telecom short codes	White listing
Interconnect CDR	2,000	1,000 GT faking	SS7 Firewall
Roaming CDR	22,000	11,000 Wrong SMSc no	SMSc Firewall
Blacklisted Numbers	1,600,000	1.3Million same GT	Enter operators comm.
IRSF Numbers	10,000	10 numbers found in Bill complain	Block at gateways
One Local number CDR	31,624	4,225 for itself	Customer behavior analysis
SMS content	476	476 sent to app.	Content filtering

3.3.2. Pattern detection

Patterns extracted from Antispam data are;

a) Messages are blocked based on the keywords when the messages are sent to ethio telecom local numbers and short numbers. The messages are block while customers are sent messages to ethio telecom CS short numbers such as 994, 882. Around 14% of daily detected messages are blocked while the messages send to these short numbers.
b) Around one million messages are sent to one destination (one telephone number), the message contacts show that most of the fraudulent messages are sent to applications for instance MacAfee, OTT Services, and other advertising purpose.
c) International short numbers are found as B-number such as 0, 00, 0000, 1, 11, 1111, 1212, 1234, 08, 008, 8888, etc.
d) long number also found as receivers or B-numbers, such as 888888888888888888888
e) Finding in the internationals SMS as B-Party alphanumeric numbers such as eeee11, 56697267696e4d65646961.
f) International SMS with unknown global title.
g) Application related numbers such as MacAfee, Google messaging, facetime update numbers.ie.001 Gt +19253539035

Patterns detected from international backlisted numbers are as below.

a) Out of 1.6 total blacklisted numbers 403 (29 unique) international short numbers are black listed but only zero (0) is blocked in both sides, which means only while someone try to send a message to number 0 is blocked in both side as originator and as a receiver. All the other numbers are blocked only as SMMO B means the messages are blocked only when they try to send a message.

Table 9 Blacklisted number patterns

International GW Blocked numbers			
Number type	Count	Unique prefix count	Description
Short cods (1 to 9 digits)	403	29	SMMO B number blacklist, SMMT B number blacklist and NULL for (0)
			SMMO A number blacklist
Long number (14 to 20 digits)	13	3	SMMO B number blacklist
international numbers	561934	197	SMMO B number blacklist
	1059980	1	8823 (SMMO B number blacklist)
Total blocked numbers	1622330	230	Total Unique prefix

b) 1.1 million number are blocked from one prefix +8823. These prefixes contain on third of the total blacklisted it required further analysis, because the number is not found in the international high-risk range list.
c) A total of 230 countries unique prefixes are found

3.4. Chapter summary

SMS fraud related data are many in nature, to collect the data from ethio telecom efforts are made to do not miss fraud related information. Informal discussion with domain experts and, work arounds are the techniques used to understand the domain area. The data are collected from different ethio telecom systems which are different in nature. The data includes documentation, international and local agreements, CDR and subscriber related information. Based on the analysis made on the data different patterns are extracted.

4. Chapter Four: Proposed Solution

On this chapter, SMS fraud mitigation taxonomy is constructed and discussed. The first part of the chapter considers detail taxonomy construction processes. The second part explain SMS fraud mitigation taxonomy building blocks. The last part of this chapter discussed about the refined SMS fraud mitigation taxonomy and the final part of the chapter is conclusion.

4.1. SMS fraud taxonomy construction process

The taxonomy is construct based on the process design on Figure 4.1:1; The process has four main procedural points which are **Theoretical analysis, Empirical analysis, Refinement**, and **Evaluation**. Theoretical analysis and empirical analysis are the first procedures for this taxonomy construction process. Both are discussed in previous chapters (Chapter Two and Three).

The theoretical analysis outputs are SMS fraud taxonomy and matrixes. Which are used as an impute for taxonomy refinement with empirical analysis results. The final phase of taxonomy construction process is taxonomy refinement. The final phase is evaluation and it discusses on Chapter Five.

4.1.1. Taxonomy construction methods

Two taxonomy construction methods are followed for this research [14, 9], which are using question and answer and cause and effect methods. There is no common taxonomy construction process in engineering is found**Invalid source specified.**. Only few practices in software engineering and information security related researches are found, one of them is "New comprehensive taxonomies on mobile security and malware analysis" by Canbek et al [14], who follow a question and answering method. They developed a new leveling scheme for enumerating taxonomy contents. Their naming contents from top to bottom as: Class➔ Subclass➔ elements ➔ sub elements➔ attributes➔ sub attributes➔features➔ sub features. They refer all of them are as nodes and their taxonomy is constructed with a total of 3000 nodes. Their nodes are constructed as: Attack➔ Incidents➔ Malware➔ Threats➔ Vulnerability➔ Security. On their taxonomy a summary of security related researches from 1993 to 2015 are referred and, for a graphical image they used mind map design.

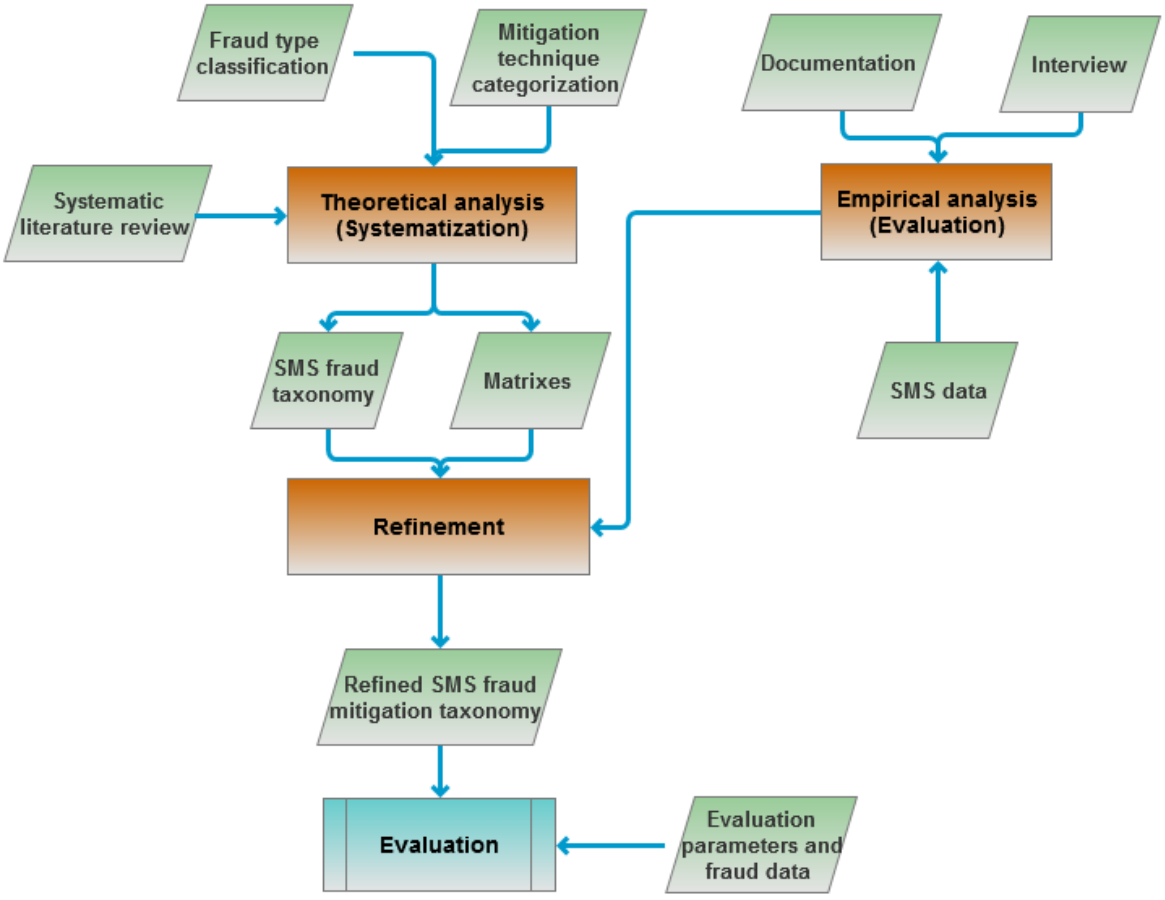


Figure 4.1:1 SMS taxonomy construction process flowchart

For this research, a question and answering method is applied, to leverage the main concepts in the SMS ecosystem. It also helps to gain all the required information on the domain. Similarly, this approach offers systematization of elements in a specific domain and it helps to enumerating taxonomy contents. For a graphical design also Mind map technique is implemented, because it is an essential tool to describe hierarchical concepts [14, 15, 50].

The second method is a cause and effect method these methods is used by many taxonomies one of them is "SoK: Fraud in Telephony Networks" Merve et al. which propose voice calls fraud taxonomy. The cause and effect method help to make the taxonomy clear and easy to understand. The taxonomy has five cause and effect categories i.e. **root cause**, **weakness**, **techniques**, **fraud schemes** and **fraud benefits**.

For this research, Cause and effect method is adopted to have a comprehensive view of SMS fraud ecosystem, to make the taxonomy clear and easily understandable. Also, to make the SMS fraud mitigation techniques manageable based on the holistic approach.

SMS fraud mitigation taxonomy has four main nodes, namely technology, vulnerability, fraud and mitigation. these main nodes are constructed using cause and effect and question and answer methods. the cause and effect method is used as the technology vulnerability is because of the hole on the technologies, and the fraud is committed based on the vulnerabilities and the mitigations are the effect of the fraud.

The question and answer method is used by assigning a different question for each main node i.e. Technology (Which), Vulnerability (Where), Fraud (How) and Mitigation (What). What type of technology is used for SMS, where is the vulnerability of the technologies, why fraud committed, and How the mitigation techniques are applied. Each main node has three sub technological categories which are Network/Protocol technology, Service technology and Actor technology.

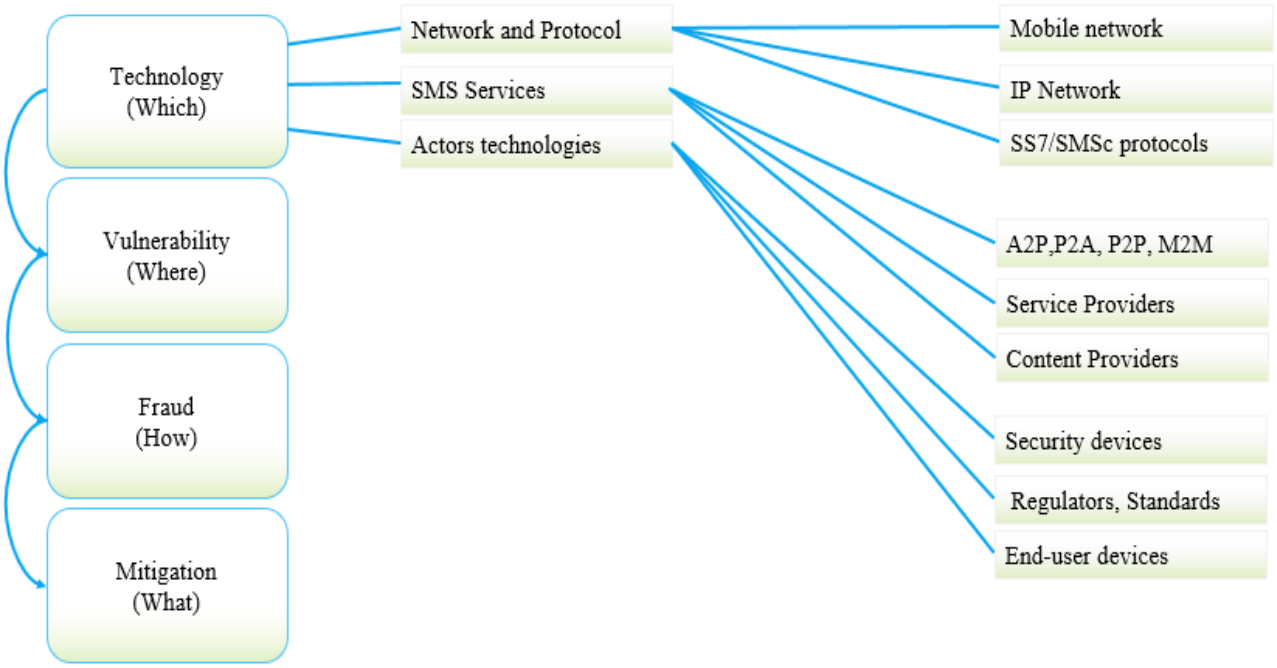


Figure 4.1:2 SMS fraud taxonomy High level design

4.2. SMS technology (Which)

SMS technology domain is constructed based on the what question. Which type of technologies do SMS service use. The technology sub nodes are labeled as Network/Protocol, Service and Actors. These sub categories are defined until all the technologies are classified under its domain. The classification method is:

Global-node→Technology→Sub-technology→Tech-element→Sub-element→Tech-attribute→Sub-attribute

Network/Protocol Node: The nodes divided in to three main nodes which are IP, Mobile networks and protocol. The IP network has only one sub node which is External Short Message Entities (ESME). ESME network structure is also discussed on literature review chapter. Messages comes from ESME are directly goes to SMSc so that the detail is explain under SMSc network. Mobile node has four sub categories which are Global System for Mobile (GSM), Unified Mobile Transmission System (UMTS), Long Term Evolution (LTE), SMSc and signaling network (SS7) networks Figure 4.2:1.

Th protocol node by itself has three sub nodes Signaling, IP and Messaging. Signaling protocols are SCCP, MTP TCAP and MAP [19]. They are used to send and received SMS data by checking the Global title of the sender, addressee matching technique. SMSc Protocol Node as sender SMSc is responsible for end to end message transformation the protocols have many responsibilities [3], Shot Message Peer to Peer (SMPP), and IP network protocols.

SMS-ecosystem→ Technology (What) → Network/Protocol→ Mobile→ GSM→ MSC→ AUC→ Verification

Service node has two major nodes operators and, service type. service operators consist service and content providers including different type SMS services. Service types are person to person, machine to machine and application to person. A2P/ P2A service node has five different type of services which are two factor authentication (2FA), informational messages, Advertisement, Notification, and Transaction Automatization Number (TAN). Under 2FA One Time Password (OTP) and Mobile TAN.

Actor Node; actor class consists five sub nodes which are consumers, subscribers, manufacturers, regulatory and industry forums. The sub nodes are classified in to its detail nodes. Consumers referred to who are delivers security systems and equipment's such as Firewall, FMS [8]. Subscriber contains all the service users. Manufacturers for this context are end users' device (such as mobile phone, tablet and other) producers. Regulatory referend to organizations such as ITU-T, governments, and patent organizers and industry forum contains all telecom related organizations.

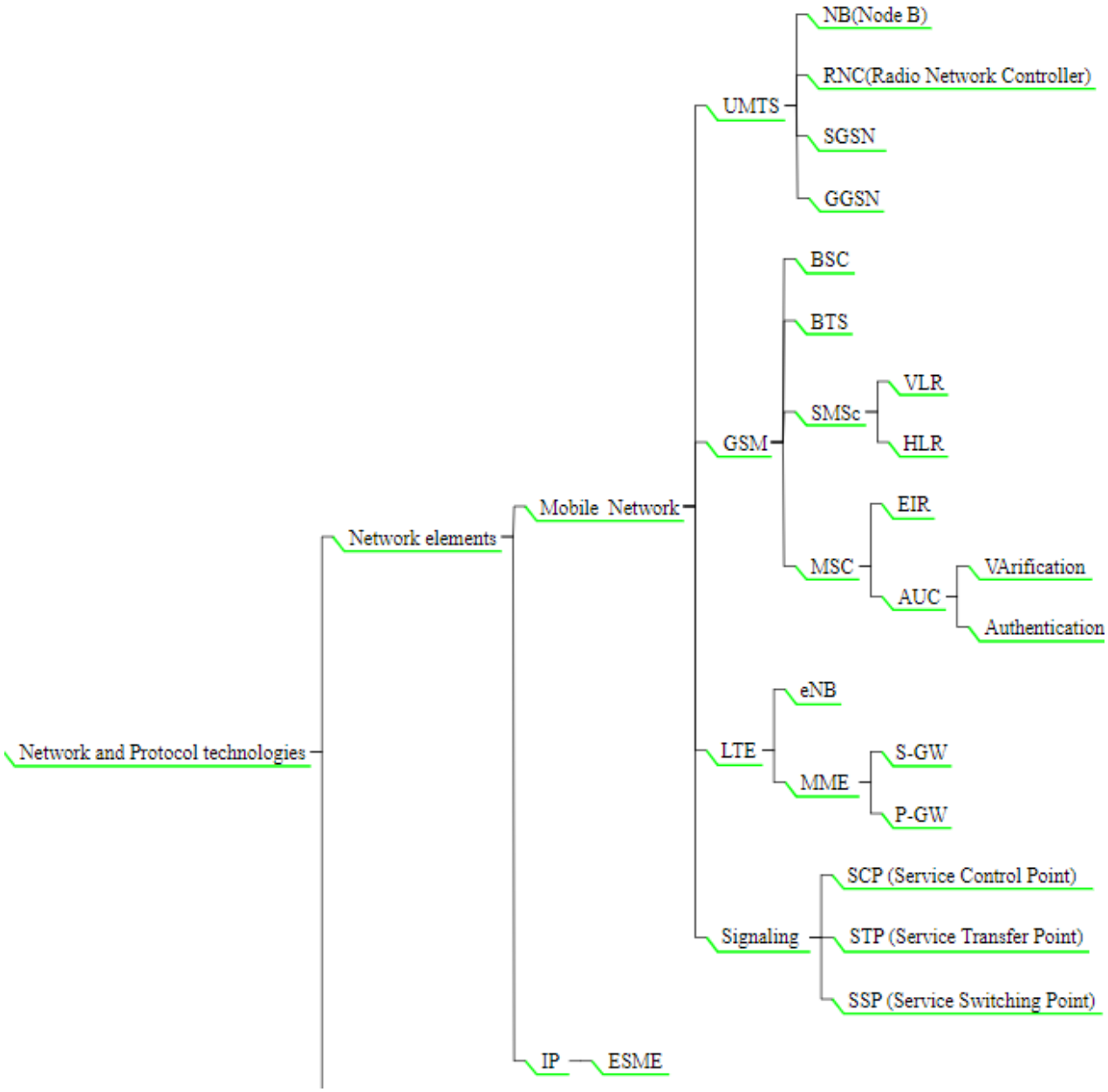


Figure 4.2:1 Mind map representation of Network/Protocol Taxonomy)

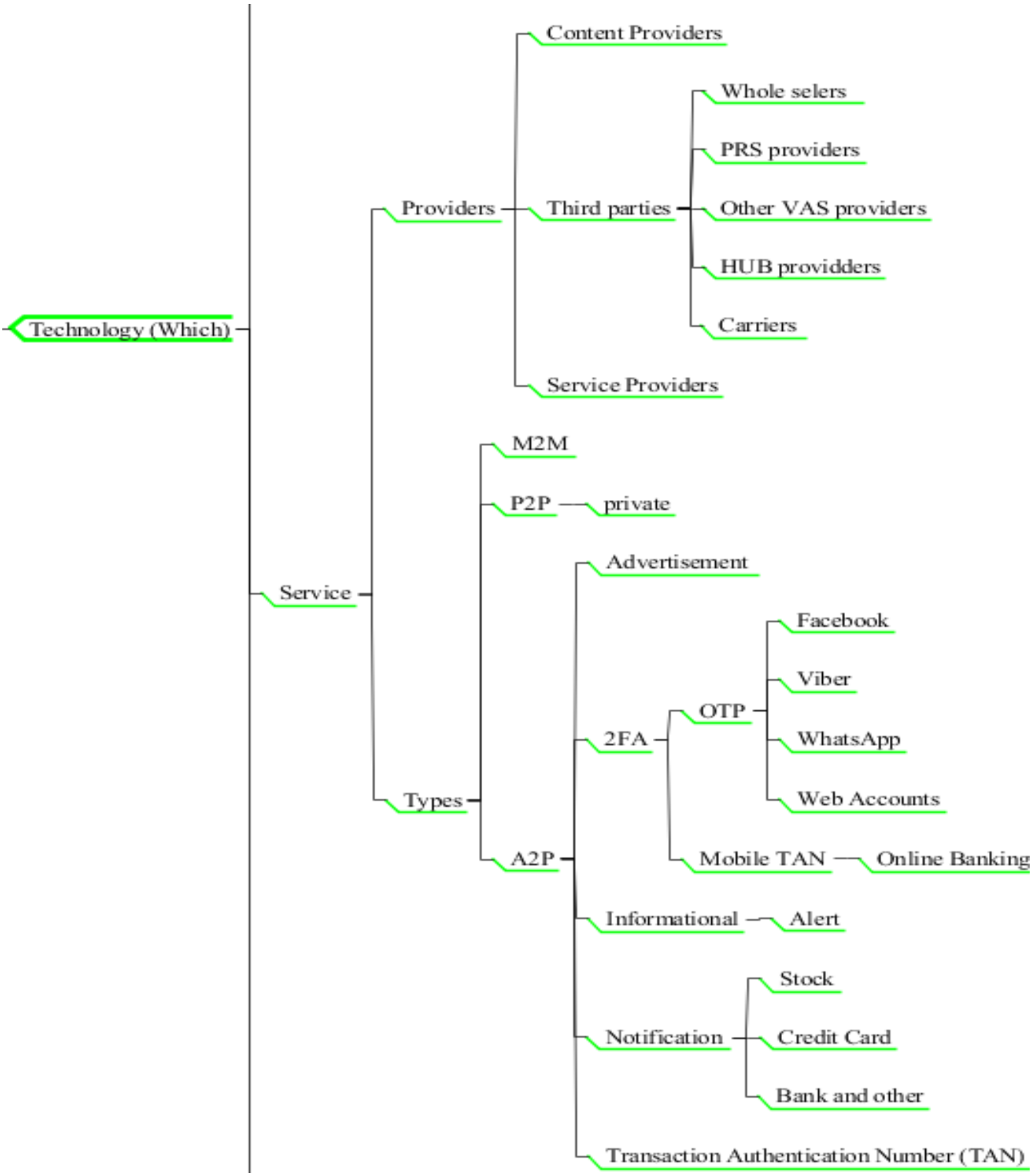


Figure 4.2:2 Mind map representation of Service node Taxonomy

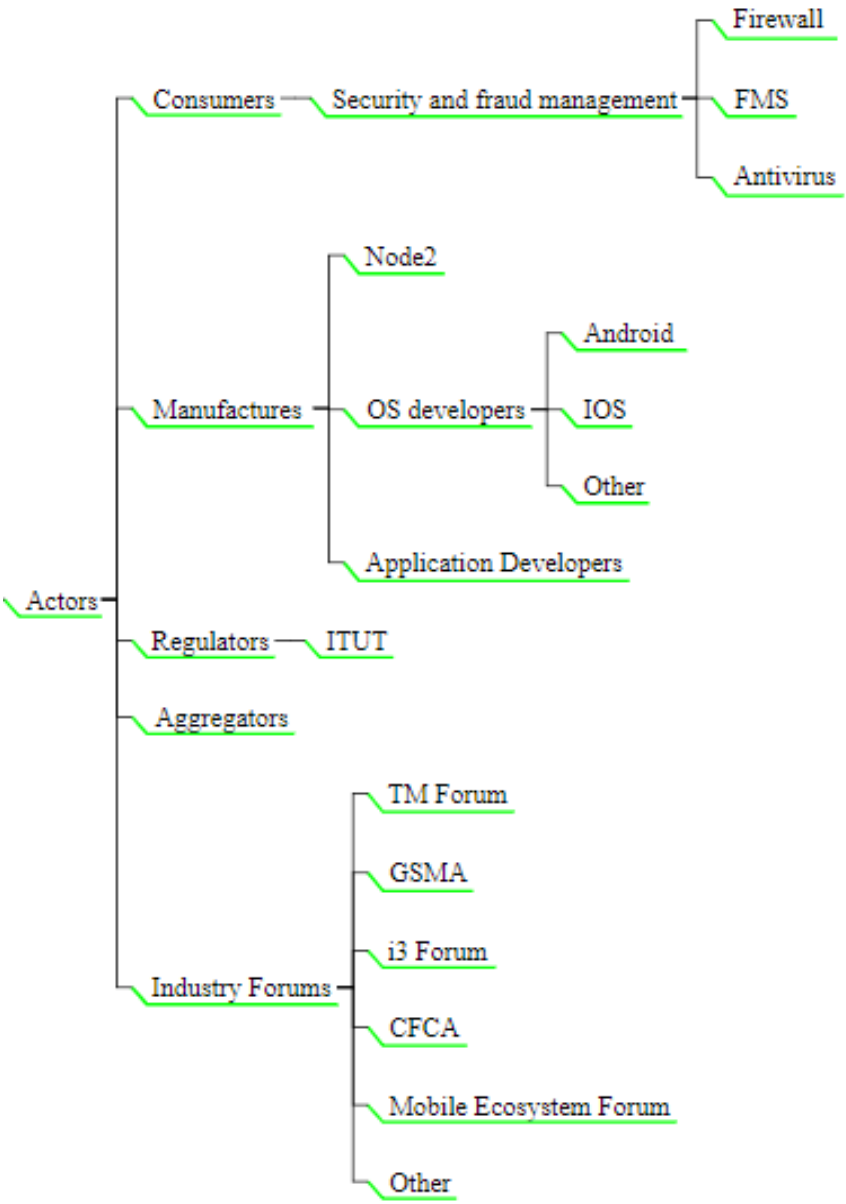


Figure 4.2:3 Mind map representation of Actor Taxonomy

4.3. Vulnerability (Where)

This node refers the weakness of the technologies listed in Section 1.1.1 and has four major nodes: Network, Protocol, Service and Actors.

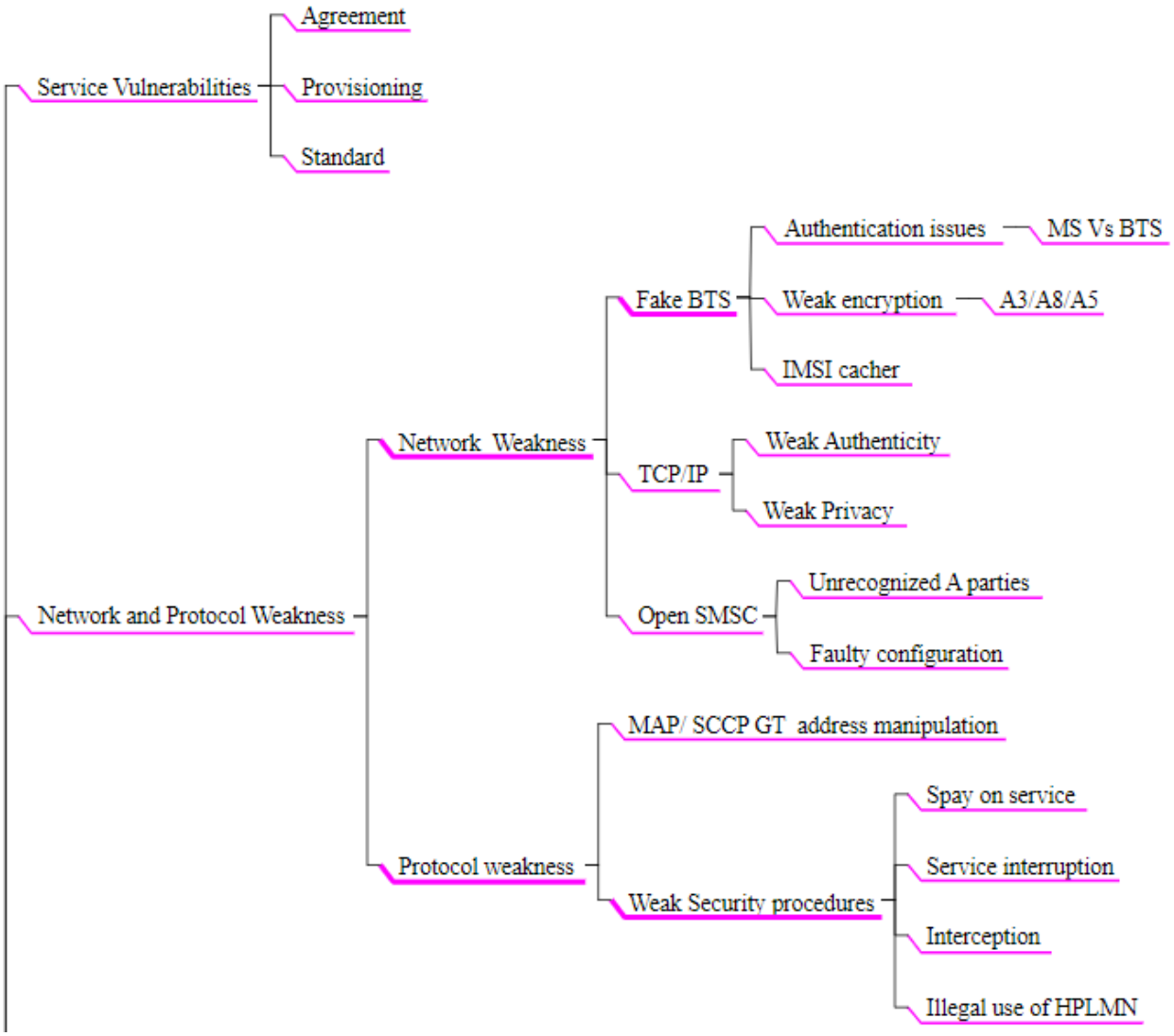


Figure 4.3:1 Mind map representation of Network and Service Weakness Taxonomy

Network and protocol vulnerabilities: telecom network is vulnerable for different type of attacks because of interoperability of new technologies with existing technology without impact analysis. The existing technology is not ready to make secure the new technologies because when telecom network deployed security was not an issue. The network vulnerability node has three major sub nodes which are FAKE BTS, IP network weakness, and SMSc weakness. Fake BTSs are deployed when the operator networks are not secured [3].

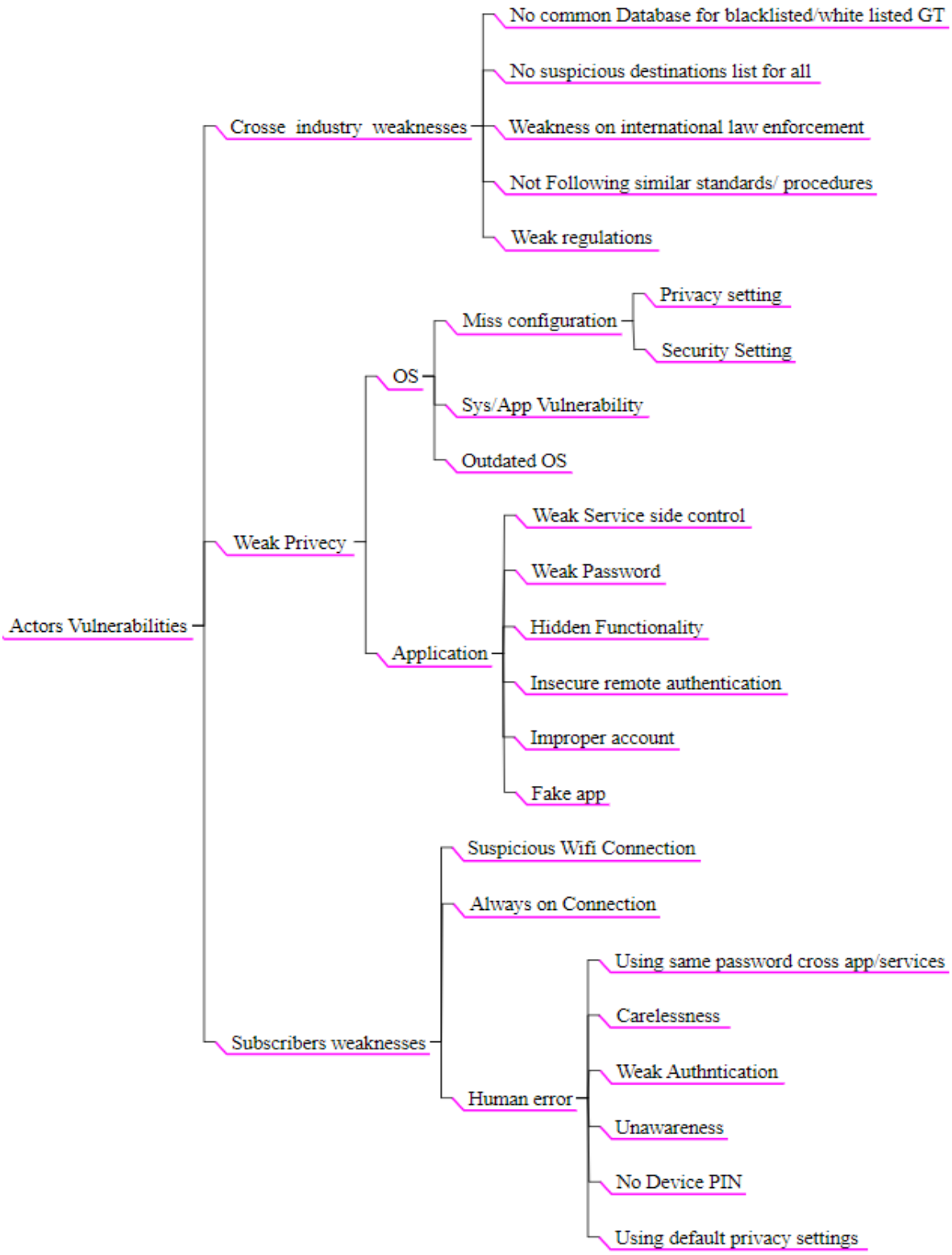


Figure 4.3:2 Mind map representation of Actor Weakness Taxonomy

Protocol Weakness: Protocols are vulnerable at different networks and network parts. In this section the protocol weakness node is categories which are security procedure, signaling protocol weakness and SMSc protocol weaknesses.

Service Weakness: Service vulnerabilities are occurred during or after launching the service. Vulnerability may come from operators, or third parties. All service types are also vulnerable; P2P messaging is vulnerable by A2P message senders by abusing service agreements.

Actor Weakness: Actor node is classified as Consumers, Subscribers, Manufacturers, Regulatory and Industry Forums. Some of actor weaknesses are weakness on security devices such as Firewalls, FMS, Mobile OS and application security holes, weaknesses related to subscriber technology knowledges.

4.4. SMS fraud (How)

To identifying SMS fraud types industry forums fraud classification documents and different literatures are reviewed. For fraud categorization 27 different literature SMS fraud classification and definitions are used. After document revision SMS frauds are categorized based on their technique, impact and behavior [43, 6]. SMS fraud types, fraud categorization and description are demonstrating in Table 10.

Factors leading to telecom fraud are many, some of them are failure to understand the complexity of new technologies, dissatisfaction of employees, weakness in operation systems, irresponsible business models and criminal greed, money laundering, political and ideological factors, ineffective audit system and free financial gain [31, 54].

SMS Bypass: Grey route, Artificial Inflation of Traffic and SIM farming are similarity in their technical implementation and the effects [6]. The technique used for those fraud is, using several SIM cards/ virtual SIMs to send or receive messages to the victim operators' network unknowingly to gain profit by not paying actual price [8].

GT Faking: Faking, MAP faking, SCCP faking, MAP & SCCP address mismatch, open SMSc, compromised SMSc, and GT scanning are grouped together. The technique used for these frauds are manipulating the sender address or A-parties' global title [35]. By doing this technique

unsecured SMSc's are found and these SMSc's are used as message center for free; the intention may to gain financial, political, or other social advantages. Most GT scan is made by looking up

Table 10 SMS fraud category

Fraud Category	Fraud Types	Description and source
SMS Bypass	SMS Bypass	'grey market' for steering messages as cheaply as possible via 'black aggregators' around the globe [43]
	Grey Route	A2P messages between mobile operators in the absence of an AA19 / AA60 agreement [8]
	AIT	When a party uses MO interconnect revenue share as a way of generating profit by sending messages to itself [6, 8]
	SIM Farming	Using a bank of SIM cards for the delivery of commercial messages [7]
GT Faking	Faking	Manipulate SCCP or MAP addresses [43, 8]
	MAP GT Faking	Manipulating a message by changing a MAP parameter [35]
	SCCP GT Faking	Manipulating a message by changing a SCCP parameter [35]
	Open SMSc	SMSCs that do not screen or validate the A-party [8]
	Compromised SMSc	Generating the fraud to reach a mobile operator SMSC at MTP level [31]
	GT Scanning	Send SMS to all Global Title address to find unsecured SMS-C [43]
SMS Spam	Flooding	A kind of spam which sent to all the users attached to the operator's network [44]
	Spam	Unsolicited message [6, 31, 16]
SMS Malware	Malware	Malicious software which affect the user and/or network [47, 55]
	Hacking	Hijack the credentials of a legitimate third party [43]
	SMs Malware	Sends SMS to premium-rate numbers without user's consent [47]
Hacking	Spoofing	Modifies the displayed number of an incoming message [31]
	Smishing	The fake message contains a URL that looks valid, or is potentially misspelled [15, 53]

through HLR address list or by generating random numbers based on global titles. generating the fraud access to the international SS7 network and by subverting a mobile operator's firewall [19].

SMS Spam and Flooding: This two fraud types techniques and impacts are similar. SMS spam are referred as a message which are not subscribed by the users, also flooding is broadcasting message to the destinations [49].

SMS Malware, Malware, and Hacking: are referred to the same attack type which is called malware. Malwares where previously attack computers and emails but currently based on the

enormous acceptance of smartphones and its functionalities malware is exist in SMS [47]. Technically SMS malware are attack the user by sending Messages to Premium rate services without users' knowledge and manipulate the attacked phones privacies.

Hacking, **Spoofing, and Smishing:** these three SMS frauds impacts are also similar, their intention is by faking the user to violate their personal information [56]. Such as credentials, social security number, bank accounts and other privet information's [48].

Based on fraud grouping discussed in Table 10 SMS frauds are categorized in five fraud types. The technologies violated to commit such frauds are Network/Protocol, Service and Actors or end devices related technologies. Figure 4.4:1 shows how technology vulnerabilities are cause to fraud schemes.

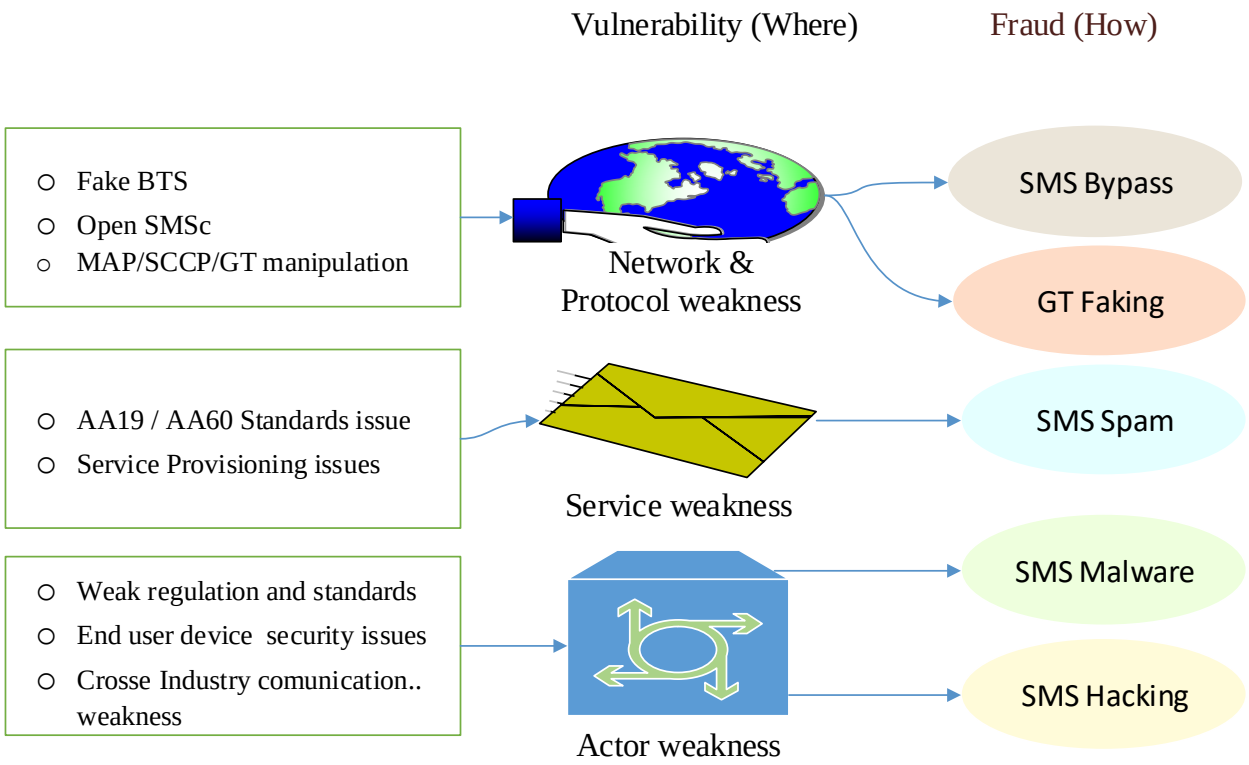


Figure 4.4:1 Vulnerability vs SMS fraud alignment

4.5. Fraud mitigation (What)

Due to the constantly changing nature of fraud, it is vital to accurately characterize and measure fraudulent events; understand how fraud is evolving; and how effectively fraud management process is taking. The mitigation techniques are required to revised periodically. In general, it is important to understand the context in which fraud is committed to take the right corrective and preventive measures [31].

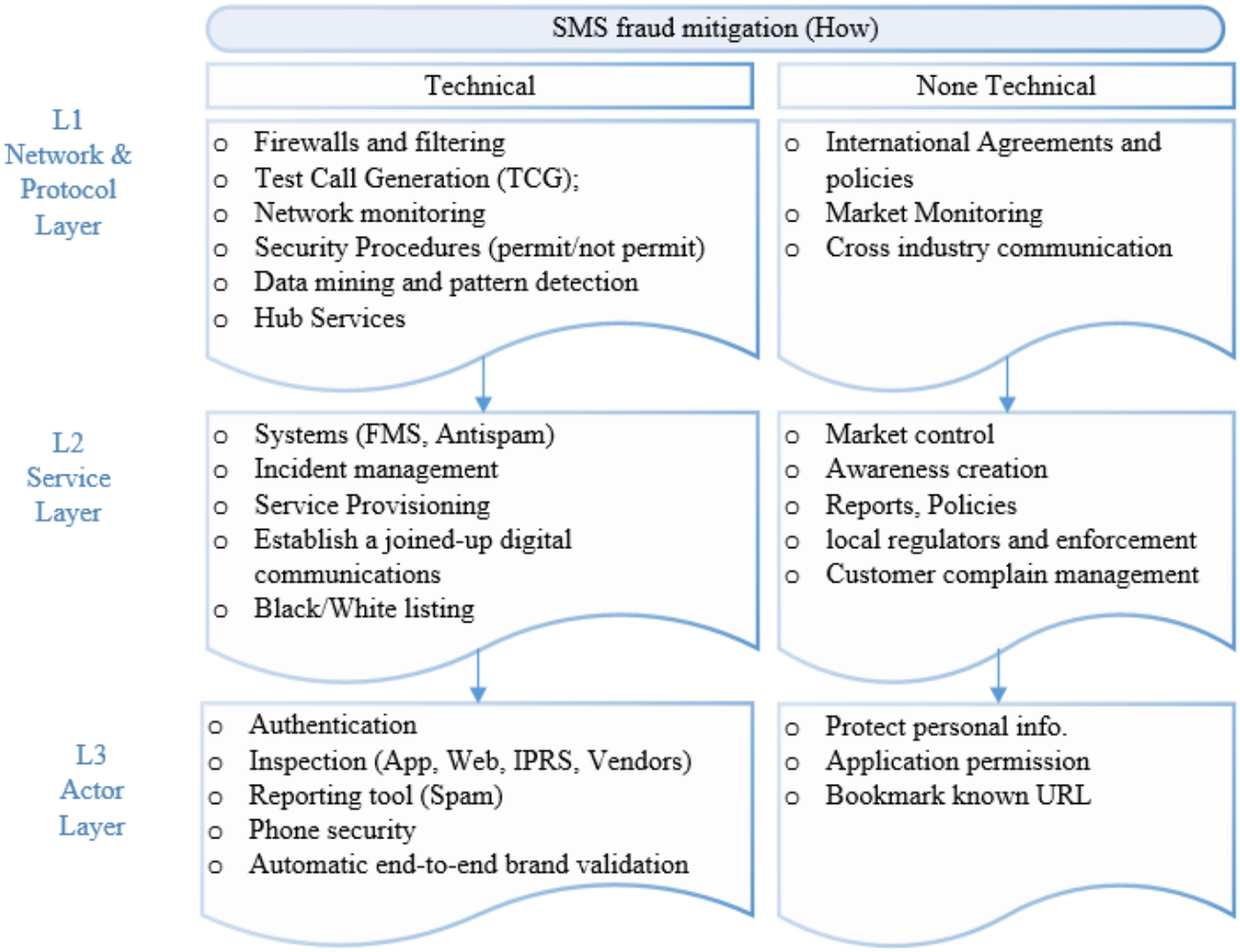
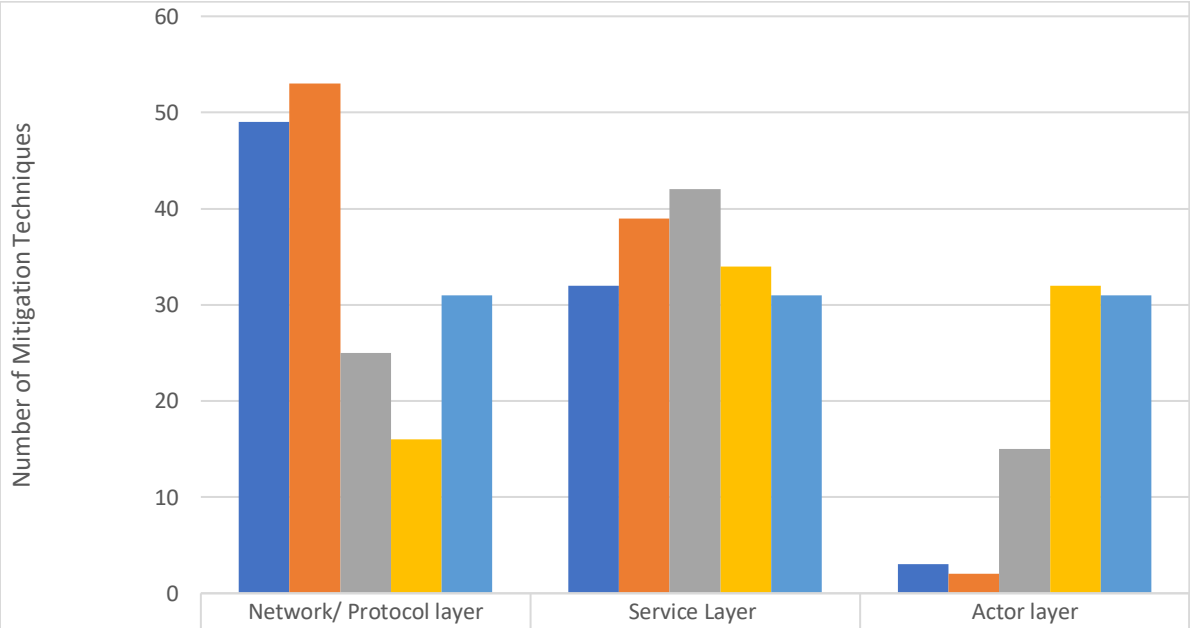


Figure 4.5:1 Fraud mitigation taxonomy in block diagram representation

Researches agreed on the importance of to have common fraud schemes and mitigation techniques classification model which widely adopted [31, 6]. GSM Association and Mobile Ecosystem Forum (MEF) fraud and mitigation techniques classification approaches are discussed in Chapter

Two Section 2.2.4. GSMA classify as technical and none technical [6]. Mobile Ecosystem Forum (MEF) also classify in four categories Network, Market, Enterprise and Consumer [8].

In this research the mitigation techniques are categorized in terms of violated and applied technology to mitigate the fraud. The mitigation techniques are classified in three technological layers i.e. Layer-1 Network/Protocol layer, Layer-2 Service layer and, Layer-3 Actor layer. Under each layer the mitigation techniques are sub categories as technical and none technical mitigation technique. Technical mitigations refers; the mitigation techniques which are applied using mitigation tool or system. The none-technical mitigations contain only policies, processes, procedures, agreements, standards, law enforcement and, alike.



	Network/ Protocol layer	Service Layer	Actor layer
SMS Bypass	49	32	3
GT Faking	53	39	2
SMS Spam	25	42	15
SMS Malware	16	34	32
SMS Hacking	31	31	31

Figure 4.5:2 Graphical representation of layered mitigation with fraud types

4.5.1. Three-layered mitigation approach

A total of technical and none technical mitigations listed are; Network/protocol layer 70, Service layer 57 and, Actor layer is 39 the lists are shown in Appendixes 6,7 and 8. The graphical representation of the mitigation techniques in each layer are shown in Figure 4.5:2.

Based on the graph on Figure 4.5:2 GT Faking and SMS Bypass got a highest number of mitigation methods from Network/Protocol layer and less number from Actor layer. SMS Spam take the highest number of mitigation techniques from Service layer and less from Network/Protocol. SMS Malware and SMS Hacking takes the highest number of actor's layer mitigations than the others.

4.6. The refined taxonomy

The refined taxonomy constructed as three by four matrix format. The horizontal path of the matrix contains the four main nodes: Technology (Which), Vulnerability (Where), Fraud (How) and Mitigation (What). The vertical path of the matrix has three layers technology/protocol layer L1, Service layer L2 and Actors layer L3. These sub technologies Network/Protocol, Service and Actors deliver common ground for all main nodes.

The mitigation part of the taxonomy sub categorized as technical and none technical mitigation under each layer. As discussed previously; technical mitigations required tool or systems with technical action and none technical are referred to process, procedures, agreements, policies including knowledgebases and awareness.

The fraud (How) part of the taxonomy related with vulnerability and mitigation as; one-to-many methods (Refer Figure 4.4:1) i.e. a single layer vulnerability may cause for many frauds and a single fraud may mitigate by different layers mitigation techniques.

The main purpose of the taxonomy is to improve current SMS fraud mitigation implementation. Currently different type of mitigation techniques is proposed and deployed. One of the limitations on mitigation effectiveness is the mitigation techniques implementation, fraud dynamicity and limitation on knowledge on fraud root causes. The propose taxonomy gives a holistic view on SMS fraud ecosystem and the mitigation techniques are classified in layers. To mitigate the fraud based on the impacted technology while the fraud committed.

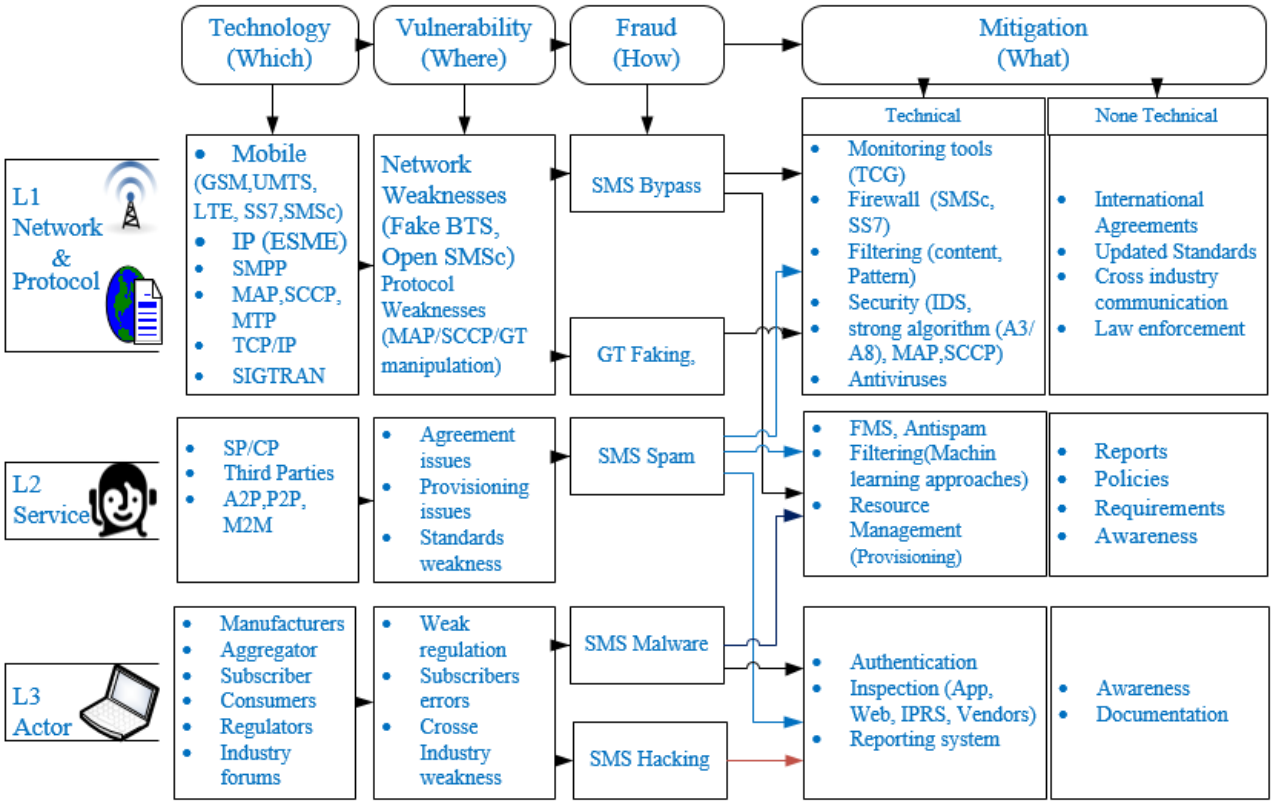


Figure 4.6:1 The refined SMS Fraud Mitigation Taxonomy

4.7. Chapter summary

On this chapter a taxonomy construction process is followed to build SMS fraud mitigation taxonomy. The proposed taxonomy is constructed as a three by four matrix form. The vertical nodes contain three-layer technologies i.e. Network/Protocol layer L1, Service layer L2, and Actor layer L3. The horizontal path of the matrix contains four main nodes Technology (Which), Vulnerability (Where), Fraud (How), and Mitigation (What). The taxonomy is constructed by using Cause-and-effect and question-and-answering methods.

5. Chapter Five: Evaluation and Discussions

In this chapter, by considering the empirical data collected from ethio telecom, the proposed SMS fraud mitigation taxonomy is evaluated and discussed.

5.1. Evaluation

The evaluation approach is adopted from Zhou et al. [57], the evaluation process has four-main phases. The first one is evaluating the overall ethio telecom SMS fraud mitigation practice based on the proposed taxonomy. The second is test data preparation process, the third phase is set evaluation criteria based on the recommended mitigation techniques to evaluate the selected data and the final step is evaluation result and discussion.

5.1.1. Evaluating ethio telecom SMS mitigation practice

Evaluate ethio telecom SMS mitigation practice with the proposed solution layered mitigation approach, i.e. Network/Protocol, Service and Actor layers refer Figure 5.5:1.

Ethio telecom use Antispam system as active SMS fraud mitigation tool which detect the message based on the preconfigured key words. Ethio telecom deploy fraud management tool but because of source data problem it is not functional for SMS frauds. The other method is through bill complain, bill complains are collected and examined by fraud experts if the complaint is related to fraud. If this numbers suspected, then the numbers will be blacklisted/blocked at international gateways and soft switches. The other method is collected customer complain from hot line 994 and analyze the complaint and take appropriate action.

To prevent international SMS frauds ethio telecom follow AA19 / AA60 agreement with Roaming partners and HUB operators [43]. GSMA operators' reference documents and ITU-T standards are used for such agreements.

The other protection method is network monitoring tool. The monitoring tool generate alarm if any unusual traffic exists. The MO or NT number found in unusual traffic is blacklisted at

international gateways of ethio telecom after further analysis is performed. In addition to these internationally confirmed high risk destination numbers also blocked at international gateway.

Service provisioning and market analysis are also performed in ethio telecom through fraud management tools and through policies. Such as SIM card distribution policy. Based on the analysis result ethio telecom didn't use all the mitigation techniques which are usually used in many operators [6].

5.1.2. Evaluation setup

A. Select 100,000 SMS fraud records sample numbers:
    - 80,000 SMS fraud numbers CDR records from antispam system detected numbers of July 17 to July 23, 2018.
    - 20,000 SMS fraud CDR records from PRM and CRM systems (SMS fraud numbers detected through customer complains)
B. Collect 10K international high-risk destination numbers from GSMA August 2018 reports.
C. Collect all blacklisted data which are collected from soft switch (1.6 million numbers)
D. July 17 to July 23, 2018 SMS traffic and antispam protected numbers charts

5.1.3. Evaluation procedures

The possible mitigation techniques are listed on Appendixes 6,7 and 8 but, for this evaluation only the mitigation techniques which doesn't require a specific system are applied. Data extraction and filtering is done through PLSQL scripts.

5.1.3.1. Network/Protocol Layer evaluation and result

Selected mitigation techniques:

a) Monitoring SMSC Global Title, or A_MSISDN is wrong [35]
b) No alphanumeric support on networks [8]

c) Monitor large number of messages being sent to one or more destinations [35]
d) Permit only long numbers until a customer proves that they are who they say they are [8]
e) Evaluate illegal use of the HPLMN SMS-C by a third party [7]

Table 11 Network/Protocol layer evaluation result

Sample SMS Fraud numbers CDR	Network/Protocol layer technical mitigations evaluation					
	Number of records filtered per mitigation technique					
	a	b	c	d	e	Total
100,000	1,232	140	63,248	4,482	1,572	70,674

Network/Protocol layer results (Table 11)

Network/Protocol layer consists five types of mitigation techniques for evaluation, as discussed in chapter three all the collected data are inserted in to oracle database. So that the evaluation is performed by applying the mitigation technique behavior on the PLSQL query language.

The first mitigation technique is filter if any SMSc global title (International prefix) of a message or senders' number (A-Number) is wrong. To filter this first check if there is any discrepancy with in the sender CDR fields i.e. sender GT, operator GT, country code, sender number GT. And receiver operator GT, SMSc are analyzed. Then, all mismatched records of such fields are filtered, and records are counted for this case 1,232 records are found.

The second mitigation mechanism is filter if there are any alphanumeric sender/receivers found in the sample records. A total of 140 alpha numeric numbers are found as MT/MO. The third mitigation mechanism is to filter if large number of messages are sent/ received. From the total number of samples CDR 63,248 messages are sent from one destination. And the mitigation technique in the last column require to filter there is any short number can send/receive international SMS. Short number refers from one-digit to five-digit numbers. 5482 short numbers are found which received SMS successfully. The total result shows from 100,000 records 70% of them can be filtered at network/protocol layer.

f) Monitor capricious loads on the network due to bulk SMS [8]

g) Trigger alarms to indicate increased traffic flows over the network [6]

h) Establish or enhance the incident management capabilities to be able to respond to incidents in the core network domain [35, 7]

The mitigation techniques listed from (f), (g), and (h) are based on the traffic flow graph on Figure 5.1:1 and Figure 5.1:2.

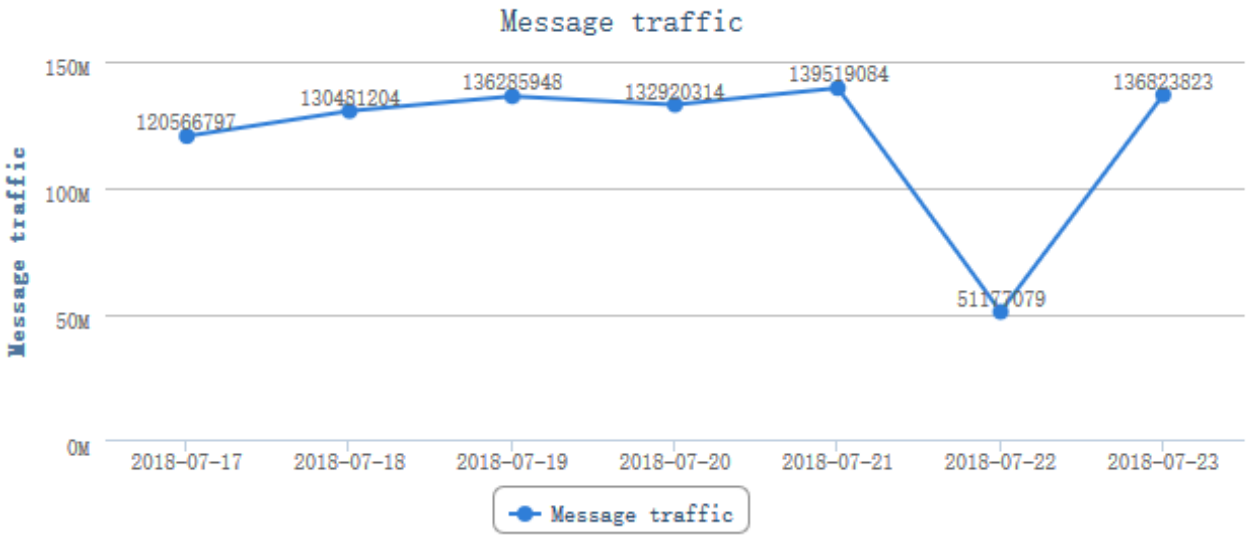


Figure 5.1:1 ethio telecom SMSc one-week traffic July 2018

SMS traffic is drop from 140 million 2018-07-21 to 51 million 2018-07-22. Then back to 137 million on 2018-07-23. It is around 1/3 usual traffic is off in one day. Therefore, in the network side ethio telecom required to analyze the reason of the traffic goes to 140 million (if it is normal traffic, spam traffic, or flooding is happened) is a normal traffic. Network monitoring system with automatic alarm generation tool. And incident management capability.

In addition to that, when one-week ethio telecom SMSc and Antispam system traffic compared refer Figure 5.1:1 and Figure 5.1:2. The actual SMSc traffic is dropped in July 22, 2018 by one third of usual traffic i.e. from 140 million to 5 million but the antispam system detection on the same date is similar with other days refer Figure 5.1:2. i.e. the usual blocked message trend of the week is around 1.2 million and in July 22 also block 1.1 million messages.

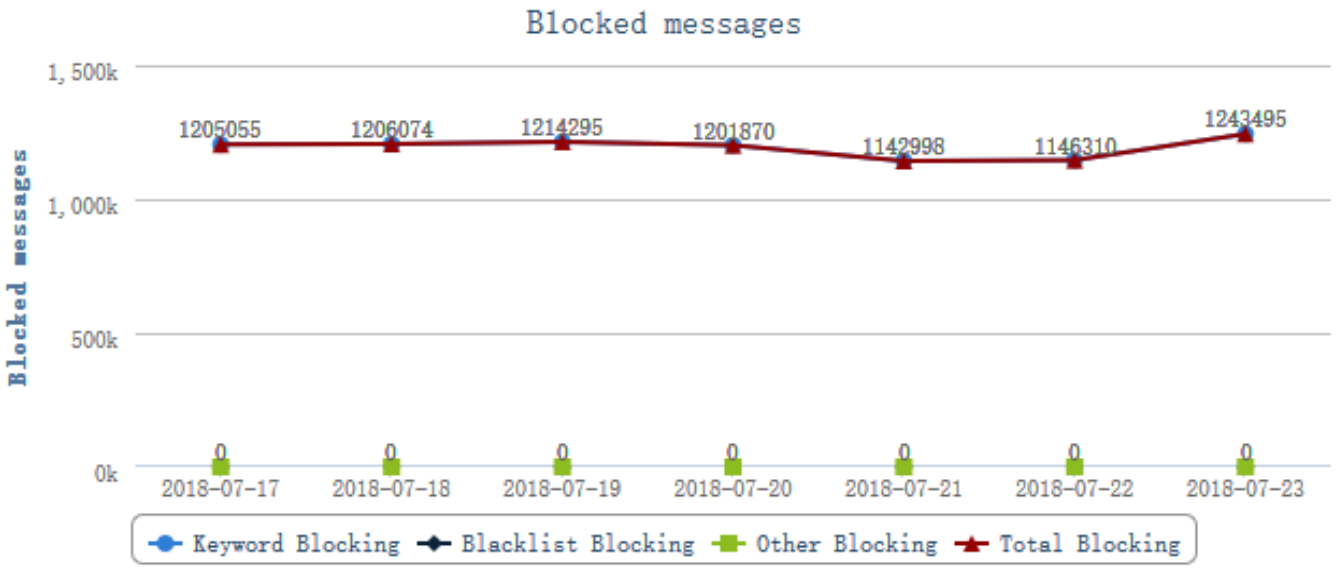


Figure 5.1:2 ethio telecom Antispam system one-week detection traffic July 2018

5.1.3.2. Service layer evaluation and result

Selected mitigation techniques

a) Blacklists, Whitelists [15, 7]
b) Monitor unusual patterns of usage of SMS messaging per customer [8, 6]

Table 12 Service layer mitigation evaluation result

Sample SMS Fraud numbers CDR	Service layer technical mitigations evaluation		
	Number of records filtered per mitigation technique		
	A	b	Total
29,898	13,900	3,225	17,125

Service layer result (Table 12)

From 29,898 sample SMS CDR 13,900 messages are sent to local short codes which are 994, 822, and 824. Most of the records are blocked by antispam system based on the pre-configured keywords. These messages are containing the same keyword, but the messages are blocked unintentionally, because the purpose of the message filtering P2A messages. Which are messages

that send automatically by preinstalled malicious applications without user knowledge. So, if ethio telecom use white/blacklisting in Antispam system these messages were not blocked. The second is unusual pattern detection, one number sent 3,225 messages for itself within one day. Therefore, out of 29,898 SMS fraud records 17,125 records can be mitigate by the selected service layer mitigation techniques.

c) Create and share a global blacklist of companies/ numbers [12]

To share blacklist companies or numbers, there is no globally accessible blacklist database, but there is a trend that operators create its own blacklist databases to monitor fraudster companies. Industry forums also collect hotlist numbers from operators, then the number will be communicated to all the operators through email, or on forum websites.

Therefore, ethio telecom also can create its own backlist company's database also, share to industry forums high risk numbers. The benefit get from this action is the number are internationally consider as a fraud and the bill related to these confirmed high-risk number is released. Also, the owners are communicated accordingly, and it is helpful for lawful enforcement.

5.1.3.3. Actor level evaluation and result

Mitigation techniques

a) Install genuine applications provided by trusted vendors [56]
b) Monitor and report if any un used bill [8]

Table 13 Actor layer mitigation evaluation result

Sample SMS Fraud numbers CDR	Actor layer technical mitigations		
	number of records filtered per mitigation technique		
	A	b	Total
12,773	4,492	6,200	10,692

Actor layer mitigation result on (Table 13)

The first mitigation used is to install genuine applications from known sources. These types of SMS malware prevention method are preferred in many literatures, if applications are only installed from known stores, i.e. for android OS, applications only from Google play stores, but Google store only use user rating and permeation-based protection. But IOS/ apple phone applications are inspected before allowing for user installation.

Some telecom service providers protect their customers by blocking the application in their network, by educate their subscribers about malicious applications, and by reporting application to remove from application stores.

From the total 12,773 SMS fraud CDR 4,492 messages are sent to applications without user knowledge, and 6,200 messages are sent to different high risk IPR numbers without user knowledge (found in bill complain CDR). The messages are sent consequentially from different numbers to one IPR numbers.

The third mitigation mechanism is to report the spam message originator to short numbers or operator hotline. Operators configure dedicated spam reporting mechanisms such as; configure a short code for spam reporting, or dedicated website for URL/DNS reporting. As soon as the user received a spam message automatically send the spam number to short code so that the operator easily monitors spammers. It is the same for the web-based reporting. In our case 1, 200 records are call back SMS messages and the users replay for these messages. In actor layer mitigation from the total 12,773 messages 10.692 are detected based on the filtering methods.

c) Report the suspected /Spam message to a short code [5,20]
d) Re-configure phone settings [5]
e) Black list and remove malicious application [4]
f) Secure a mobile device by a password and other access control methods [20]
g) Block messages unregistered or unauthorized originators [5]
h) Monitor and report if any un used bill [13]

Awareness creation is important to mitigate most actor layer SMS attacks. Some mitigation techniques are re-configuring phone settings such as update the OS to the latest version. Remove malicious applications, using strong credentials for access control mechanism. Block unknown messages, bookmark recently used URL's to identify the fake senders,

5.1.3.4. Three layered evaluation results

The average mitigation performance of the layered approach from all layers are in Table 14.

Table 14 Layered mitigations evaluation results

Total SMS fraud CDR	Mitigation layers mitigation results			
	Network/Protocol	Service	Actor	Total
100,000	70,674	17,125	10,692	98,491

The evaluation results from all layers are shows from 100,000 SMS fraud CDR 98, 491 of the records are filtered by the mitigation techniques used in each layer. This implies only 2,081 records patterns are not detected by these mitigation approaches. Currently ethio telecom use detection techniques after affecting systems performances, company revenue, quality of service and end user privacy, money and trust on the service provider. So that these 98% of the messages can be mitigate by the new approach before any impact.

From the Table 17 result network/protocol mitigation reaches to 71% and service layer 17% and actor layer around 11%. But the layered mitigation techniques are applied by 100,000 starting from network layer, then the reset of the records are filtered by service layer mitigation the final is on actor layer mitigation techniques.

5.1.3.5. Limitation

- All the proposed mitigation techniques are not applied for these evaluations, because most of them are required live system.
- None technical evaluations are not considered in the evaluation.

5.2. Result and discussion

Different security related taxonomies are proposed, and taxonomies are used to characterize a specific domain [14]. There is no taxonomy on SMS fraud mitigations, but some telecom fraud related works are previously proposed, but which doesn't include the mitigation and all SMS fraud parts [9]. The proposed SMS fraud mitigation taxonomy unique characteristics are listed as follow.

- Gives a comprehensive view of SMS fraud ecosystem, using the four main nodes (technology, vulnerability, fraud and mitigation) and dividing them in to layered technological categories (Network/Protocol, Service and Actor).
- Contain the possible mitigation techniques from state of the art (literatures, Fraud management companies' whitepapers, Industry forums, Standardization companies and, SP/CP practices)
- SMS fraud categorization; i.e. 19 fraud types [43, 7, 54] are categorized in to five.
- New layered mitigation approaches (Three Layered); i.e. Network/Protocol, Service and Actor layers including technical and none technical mitigation techniques.
- Using two taxonomy construction approaches; i.e. cause and effect method [9], question and answering method [53, 14].

The evaluation results identified 98,491out of 100,000 fraudulent short message records are mitigated. This means only 2% of the detection can be detecting using current ethio telecom methods i.e. antispam or customer complain. he other are detected using the proposed layered approaches at network/protocol, service and actor layers. The proposed hierarchical mitigation can identify 98% of the fraud refer Table 14.

Different patterns are detected from empirical analysis and evaluation results; such as short numbers and alphanumeric, unbalanced transactions, fake SMSc, and other fraudulent behaviors. These patterns are detected while SMS fraud behavior analyzed, so that ethio telecom SMS network is allowed such fraudulent transactions. It implies that as the network is not protected there are other not detected SMS CDRs can be found in normal SMS CDRs.

Table 15 Comparison on results

Comparison on SMS fraud mitigation practices	
Ethio telecom trends	Proposed solution
100,000 SMS fraud records detect by antispam system and bill complain • Detected after Impacted the company and subscribers.	Out of 100,000 SMS fraud records 98,491are protected • Mitigated before any impact on company and subscribers
Usually Detection • After impact on system performance, company revenue, and customer privacy and money	**Mitigation** • Give emphasize for prevention to protect before effect
Static • Detection methods are not changed for years	**Dynamic** • Dynamically changed mitigation techniques based on the fraud scheme and technologies updates
Similar mitigation for all fraud types	**Mitigation techniques are applied through:** • Fraud root causes analysis • Examine impacted technologies • Select appropriate mitigation techniques
None technical mitigations are missed: • limitation on follow-up and take appropriate action if service abused, local and interconnect agreements are violated, misused policies and standards	**Give emphasize for none technical mitigations:** • Take proper action if international agreements, Services, Policies, Standards are violated • Inspect agreements, policies, standards, procedures, and, SLA in predefined time • Communicate with other operators and responsible parties if any violation occurs and apply law enforcements
Network is not protected for different short message frauds	**Propose a verity of network mitigation techniques such as:** • Firewall / monitoring tools at SS7/SMSc • Monitor unbalanced traffic • Protect IP networks from Fake URL/DNS • Do not allow short and alphanumeric as A or B parties in the network
Detection techniques are not effective i.e HUB service, Antispam system, FMS	**The taxonomy helps to identify appropriate solution** and effective implementation

In general, instead of detecting all SMS fraud through antispam and bill complain after many impacts. It is recommended to use the proposed solution which help ethio telecom to gain advantages from HUB service and mitigate SMS fraud before affecting the company and its subscribers.

Antispam system has the ability of black and white listing. But ethio telecom use only the keyword filtering functionality. So that ethio telecom can make the antispam system multifunctional to improve the mitigation approaches. Also making the FMS operational for SMS frauds is the other method to detect fraud early.

Preparing educational resources for employees, content providers, consumers and, subscribers ethio telecom can decrease SMS fraud trend. Because most actor layer SMS frauds such as SMS malware and SMS faking are happening because of user carelessness, and malicious application developers.

6. Chapter Six: Conclusion and Recommendation

6.1. Conclusion

SMS service is one of advanced telecom service which attack by different type of frauds. To tackle these frauds a lot of mitigation techniques are proposed, designed and implemented [27]. In this work Instead of proposing a new mitigation technique working on the effectiveness of the existing mitigation techniques.

Comprehensive knowledge on fraud root causes, a variety of new technologies, several services and, different actors are involved in the ecosystem are the main issues raised as limitation on SMS fraud mitigations [9]. The proposed taxonomy is constructed by considering these limitations.

The taxonomy is constructed as a four by three matrix, with the main nodes Technology (Which), Vulnerability (Where), Fraud (How) and Mitigation (What). Each main node also sub-categorized in to three technological layers, i.e. Network/Protocol, Service and Actor. In addition to this categorization the Mitigation (What) node classified as technical and none technical mitigations.

The proposed taxonomy is evaluated by taking 100,000 sample SMS fraud CDRs from ethio telecom different databases. The evaluation is made by applied different mitigation methods in each layer. These layered based mitigation approach mitigate 98% of the records, these implies that only 2% of the records required current ethio telecom detection approach. Therefore, using the proposed layered approach is advantageous for ethio telecom.

6.2. Recommendation

To improve the use of SMS fraud mitigation techniques, here are the lists of possible recommendations.

- Before implementing a new mitigation technique better understand the fraud root cause, the technology used, including understanding all actors evolving in the ecosystem

- Telecom operators give fraud awareness for consumers, subscribers and other actors in the ecosystem.
- Deploy appropriate mitigation technique based on fraud behavior and violated technologies.
- Fraud experts of telecom operators and fraud management companies are recommended to follow these layered mitigation implementation approach to have a better result.

6.3. Future works

- The taxonomy is designed in mind map and in block diagram form, as a future work; adding all possible topics on the ecosystem and make the taxonomy exhaustive.
- Automate the taxonomy to use as a guideline for SMS fraud mitigation.
- Automate the taxonomy evaluation process and evaluate all the proposed mitigation techniques including none technical mitigations.

References

[1] A. Acker, "The short message service: Standards, infrastructure and innovation," *Telematics and informatics*, vol. 31, no. 4, pp. 559-568, 2014.

[2] P. Crocker, "Converged-mobile-messaging analysis and forecasts," in *Giga Omni Media*, New York, 2013.

[3] G. Association, Writer, *White Paper of the GSMA on SMS evolution.* [Performance]. Coperatoryright © 2018 GSM Association, 2018.

[4] G. Patterson, "GLOBAL A2P SMS TRAFFIC TO GROW FROM 1.7 TRILLION TO 2.8 TRILLION MESSAGES BY 2022," Mobilesquared Ltd, uk, 2018.

[5] A. S. Chaudhari, *Security analysis of SMS and related technologies*, Eindhoven: Eindhoven University of Technology, 2015.

[6] GSM Association, "GSMA Fraud Manual," GSMA, UK, 2017.

[7] GSMA, "A2P SMS Bypass - Motivations, Detection and Mitigation," Copyright © 2016 GSM Association, UK, 2016.

[8] Mobile Ecosystem Forum, "A2P MESSAGING FRAUD FRAMEWORK," Mobile Ecosystem Forum, UK, 2015.

[9] M. Sahin, A. Francillon, P. Gupta and M. Ahamad, "Sok: Fraud in telephony networks," *InSecurity and Privacy (EuroS&P), 2017 IEEE European Symposium*, pp. 235-250, 2017.

[10] G. Canbek, S. Seref and B. Nazife , "New comprehensive taxonomies on mobile security and malware analysis," *International Journal of Information Security Science*, vol. 5, no. 4, pp. 106-138, 2018.

[11] CFCA, "Fraud Loss Survey | CFCA - Communications Fraud Control Association," www.cfca.org, New Jersey, 2015.

[12] CFCA Survey Group, "2017 Fraud Loss Survey," www.CFCA.org, New Jersey, 2017 .

[13] G. author, "www.telecoms.com," telecom.com, 14 9 2016. [Online]. Available: http://telecoms.com/opinion/keeping-one-step-ahead-of-sms-fraud/. [Accessed 23 1 2018].

[14] G. Canbek, S. Sagiroglu and N. Baykal, "New comprehensive taxonomies on mobile security and malware analysis," *International Journal of Information Security Science,* vol. 5, no. 4, pp. 106-138, 2017.

[15] C. Foozy, M. Feresa, A. Rabiah and F. Mohd, "Phishing detection taxonomy for mobile device," *International Journal of Computer Science Issues (IJCSI),* vol. 10, no. 1, p. 338, 2013.

[16] S. Agarwal, G. K. Sanmeet and G. G. Sunita, "Design and Development of Antispammer for SMS Spam Detection," in *PhD diss*, 2015.

[17] B. Reaves, S. Nolen , T. Dave and B. Logan, "Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways," *InSecurity and Privacy (SP), 2016 IEEE,* pp. 339-356, 22 May 2016.

[18] R. R. Chavan and S. Manoj, "Secured mobile messaging," *International Conference on Computing, Electronics and Electrical Technologies (ICCEET),* pp. 1036-1043, 21 March 2012.

[19] M. B. Savadatti and S. Divya , "Ss7 network and its vulnerabilities: An elementary review," *Imperial Journal of Interdisciplinary Research,* vol. 3, no. 3, 2017.

[20] V. K. Katankar and M. Thakare, "Short message service using SMS gateway," *International Journal on Computer Science and Engineering,* vol. 2, no. 04, pp. 1487-1491, 2010.

[21] L. Laibinis, T. Elena and P. Inna , "A formal approach to identifying security vulnerabilities in telecommunication networks," in *International Conference on Formal Engineering Methods*, Cham, 2016.

[22] P. Bagga and H. Rahul, "Mobile agents system security: a systematic survey," *ACM Computing Surveys (CSUR),* vol. 50, no. 5, p. 45, 2017.

[23] D. Howells, D. V. Scharf-Katz and S. Padraig, "TELECOM FRAUD 101:," ARGYLE DATA, San Mateo, 2010.

[24] K. H. John Shawe-Taylor, "Detection of Fraud in Mobile Telecommunications," Information Security Technical Report, London, 2009.

[25] FEDERAL DEMOCRATIC REPUBLIC O'F ETHIOPIA, *TelecomFraud Offenc.eProclamation,* Addis Ababa: Federal Negarit Gazeta, 2012.

[26] B. Richard, V. Chris and R. W. Allan, "Fraud Detection in Telecommunications:History and Lessons Learned," *Technometrics,* vol. 52, no. 1, pp. 20-33, 2010.

[27] G. Phil and H. Mark, "Classification, Detection and Prosecution of Fraud on Mobile Networks," in *Proceedings of ACTS mobile summit, ,* Sorrento, 2012.

[28] K. Souvik, J. Sanket and M. Vijay, "Evolving Early Combat Systems in Next Generation Telecom Fraud: Catch Them Young," in *IBM,* UK, 2013.

[29] Communication Fraud Control Association (CFCA), "CFCA 2013 Global Fraud Loss Survey," CFCA, Roseland, 2013.

[30] I. Mohammad, M. Akhter and A. Gulam, "Detecting Telecommunication Fraud using Neural Networks through Data Mining," *International Journal of Scientific & Engineering Research,,* vol. 3, no. 3, pp. 2229-5518, 2012.

[31] TM Forum, "GB954 Fraud Classification Guide V2.4 - TM Forum," TM Forum, New York, 2013.

[32] M. A. Shafil, S. A. Muhammad, C. Haruna, O. Oluwafemi, A.-S. Gaddafi , A. Adamu and H. Tutut, "A review on mobile SMS spam filtering techniques," *IEEE Access,* vol. 5, pp. 15650-15666, 2017.

[33] "www.araxxe.com," araxxe, 03 09 2016. [Online]. Available: https://www.araxxe.com/blog/fraud-detection/do-you-know-how-to-defeat-a2p-and-p2p-sms-abuse-.html. [Accessed 03 09 2018].

[34] A. Malhotra and B. Karan, "A survey on various malware detection techniques on mobile platform.," *Int J Comput Appl*, vol. 139, no. 5, pp. 15-20, 2016.

[35] GSM Association, "Official Document IR.70 - SMS SS7 Fraud," Copyright © 2015 GSM Association, UK, 2013.

[36] D. T. van , E. Paal, F. Boning and T. Van , "A near real time SMS grey traffic detection," in *In Proceedings of the 6th International Conference on Software and Computer Applications*, ACM, 2017.

[37] K. Yufeng, L. Chang and S. Sirirat, "Survey of Fraud Detection Techniques," in *IEEE international conference*, 2014.

[38] Syniverse, "Syniverse Risk Management," Syniverse Proprietary, UK, 2016.

[39] TM-forum, "Tmforum.org," 27 11 2014. [Online]. Available: https://www.tmforum.org/resources/standard/gb954-fraud-classification-guide-v2-4/. [Accessed 7 6 2016].

[40] H. Abdikarim, I. Subariah and Roseli, "Detecting SIM Box Fraud Using Neural Network," *IT Convergence and Security 2012*, pp. 5-69, 24 4 2013.

[41] GSMA FASG, "Fraud Manual," www.GSMA.com, London, 2012.

[42] ethio telecom, "http://www.ethiotelecom.et/," ethio telecom, 28 1 2012. [Online]. Available: http://www.ethiotelecom.et/?q=aboutus. [Accessed 20 10 2015].

[43] GSM Association, "A2P SMS Bypass Motivations, Detection and Mitigation," www.gsma.com, UK, 2016.

[44] B. Reaves, B. Logan, T. Dave, T. Patrick and B. and Kevin, "Detecting SMS spam in the age of legitimate bulk messaging," in *9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2016.

[45] N. S. Ismail and S. R. Halizah, "GENERAL ANDROID MALWARE BEHAVIOUR TAXONOMY," in *SCIENCE & TECHNOLOGY RESEARCH INSTITUTE FOR DEFENCE (STRIDE)*, 2016.

[46] A. Sadeghi, B. Hamid, G. Joshua and M. Sam, "A taxonomy and qualitative comparison of program analysis techniques for security assessment of android software," *IEEE Transactions on Software Engineering*, vol. 43, no. 6, pp. 492-530, 2017.

[47] A. J. Babu and R. V. Rahul, "Dissecting SMS malwares in android," in *Contemporary Computing and Informatics (IC3I)*, 2014.

[48] M. N. Banu, "A comprehensive study of phishing attacks," *International Journal of Computer Science and Information Technologies*, vol. 4, no. 6, pp. 783-786, 2013.

[49] S. Agarwal, G. Sanmeet and S. Kaur, "Design and Development of Antispammer for SMS Spam Detection," in *Doctoral dissertation*, 2015.

[50] D. Papp, M. Zhendong and B. Levente, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy," *In Privacy, Security and Trust (PST), 2015 13th Annual Conference*, pp. 145-152, 2015.

[51] E. Çetinkaya and . P. S. James, "A taxonomy of network challenges," *Design of Reliable Communication Networks (DRCN), 2013 9th International Conference*, pp. 332-330, 4 Mar 2013.

[52] N. Khan, A. Johari and S. Adnan, "A Taxonomy Study of XSS Vulnerabilities," *Asian Journal of Information Technology*, vol. 16, no. 2, pp. 169-177, 2017.

[53] B. B. Gupta, A. A. Nalin and E. Kostas, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommunication Systems*, vol. 67, no. 2, pp. 247-267, 2018.

[54] MEF Fraud Management team, "A2P MESSAGING FRAUD FRAMEWORK," www.MobileEcosystemForum.com, UK, 2015.

[55] L. Dua and B. Divya, "Taxonomy: Mobile malware Threats and detection techniques," *Computer Science & Information Technology (CS & IT),* pp. 213-221, 2014.

[56] B. Amro, "Phishing Techniques in Mobile Devices," in *arXiv preprint arXiv:1802.04501*, 2018.

[57] C. Zhou and L. Ziyan, "Study on fraud detection of telecom industry based on rough set," in *Computing and Communication Workshop and Conference (CCWC), 2018 IEEE 8th Annual*, 2018.

[58] J. Song, K. Hyoungshick and G. Athanasios , "iVisher: Real-Time Detection of Caller ID Spoofing," *ETRI Journal ,* vol. 36, no. 5, pp. 865-875, 2014.

[59] P. N. Yeboah, "Proposal and Implementation of An IDS for Potential SMS Spam Signaling Messages on SS7," *Master's thesis NTNU,* 2016.

[60] I. Androulidakis, V. Vasileios and P. Alexandros, "FIMESS: filtering mobile external SMS spam," in *The 6th Balkan Conference in Informatics ACM*, 2013.

[61] K. Deepa, Radhamani and P. Vinod, "Investigation of Feature Selection Methods for Android Malware Analysis," *Procedia Computer Science,* vol. 8, no. 46, pp. 841-848, 2015.

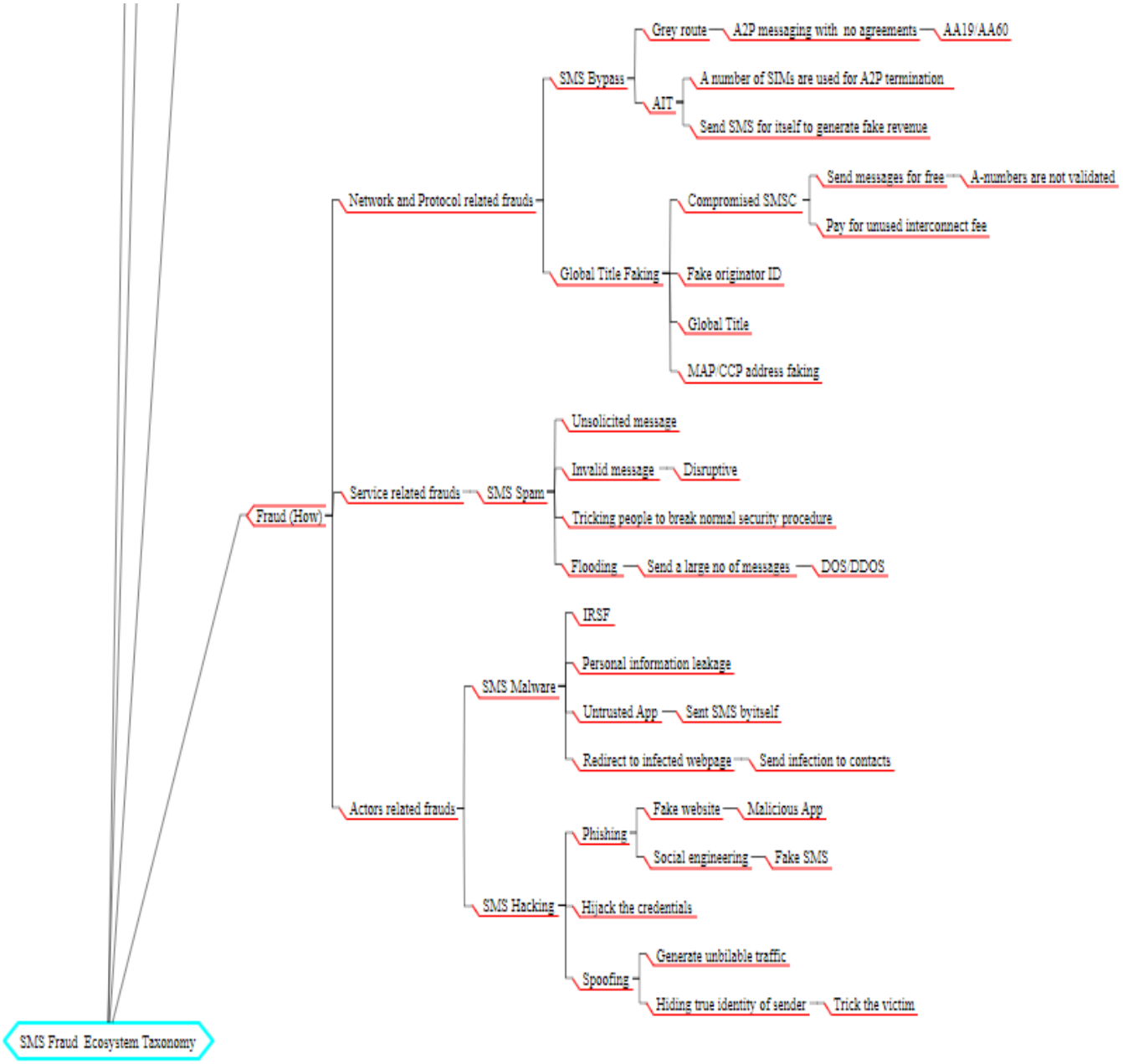
[62] A. Skovoroda and G. Dennis, "Securing mobile devices: malware mitigation methods," *JoWU,* vol. 6, no. 2, p. 7897, 2015.

[63] D. He, C. Sammy and G. Mohsen, "Mobile application security: malware threats and defenses," *IEEE Wireless Communications,* vol. 22, no. 1, pp. 138-144, 2015.

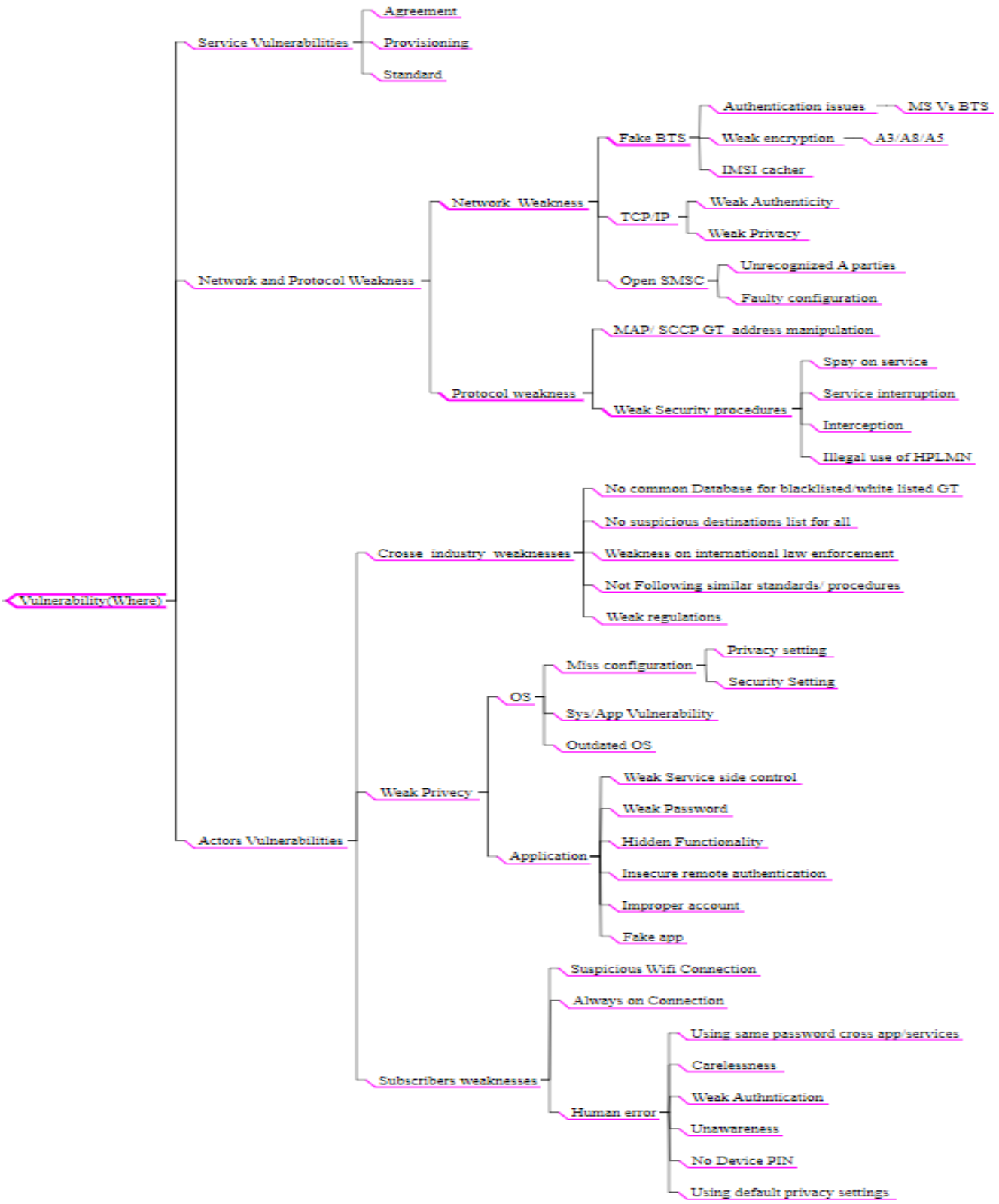
[64] M. Khonji, I. Youssef and J. Andrew, "Phishing detection: a literature survey," *IEEE Communications Surveys & Tutorials,* vol. 15, no. 4, pp. 2091-2121, 2013.

Appendixes

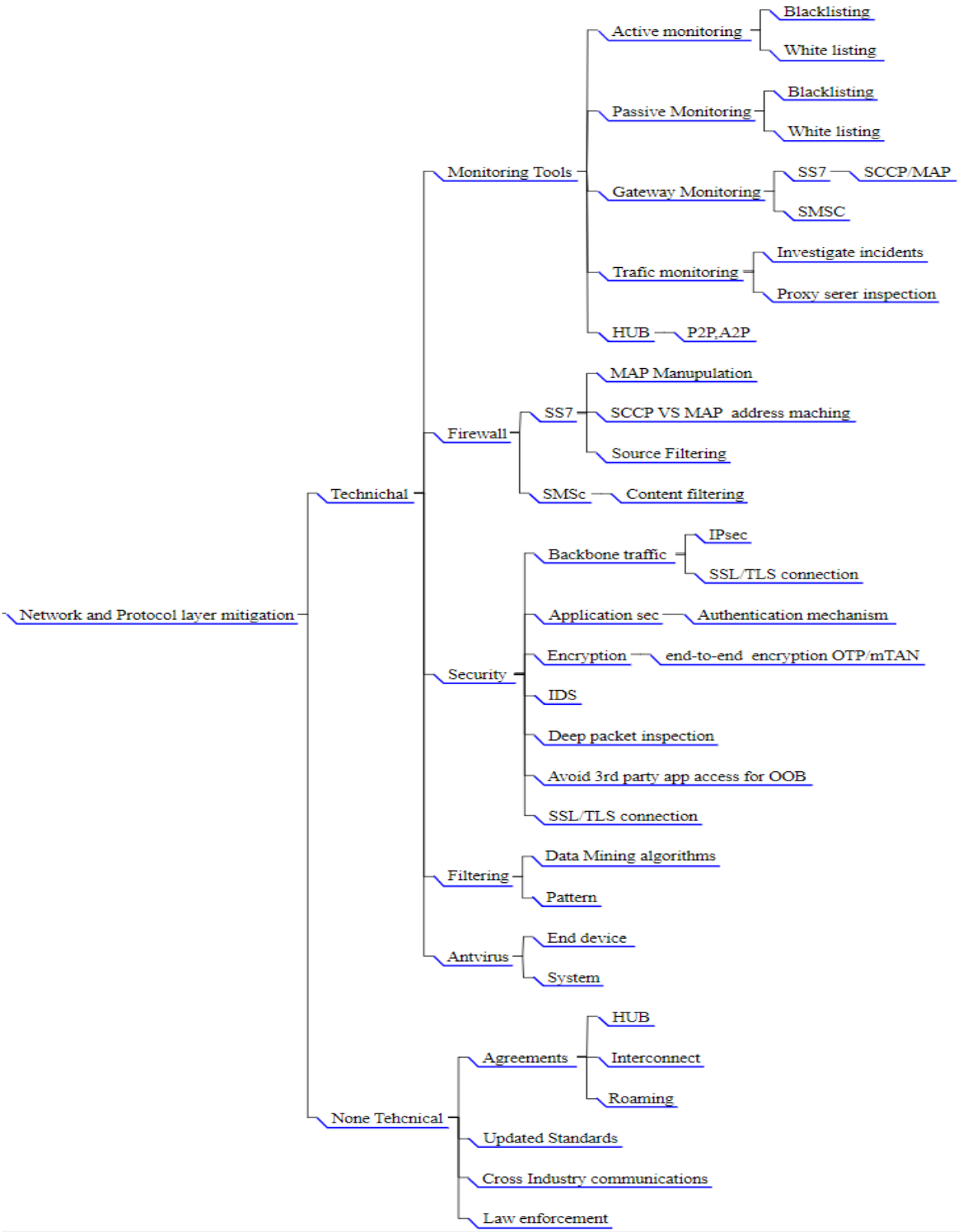
Appendix 1 SMS fraud mitigation taxonomy Mind-map design Fraud node



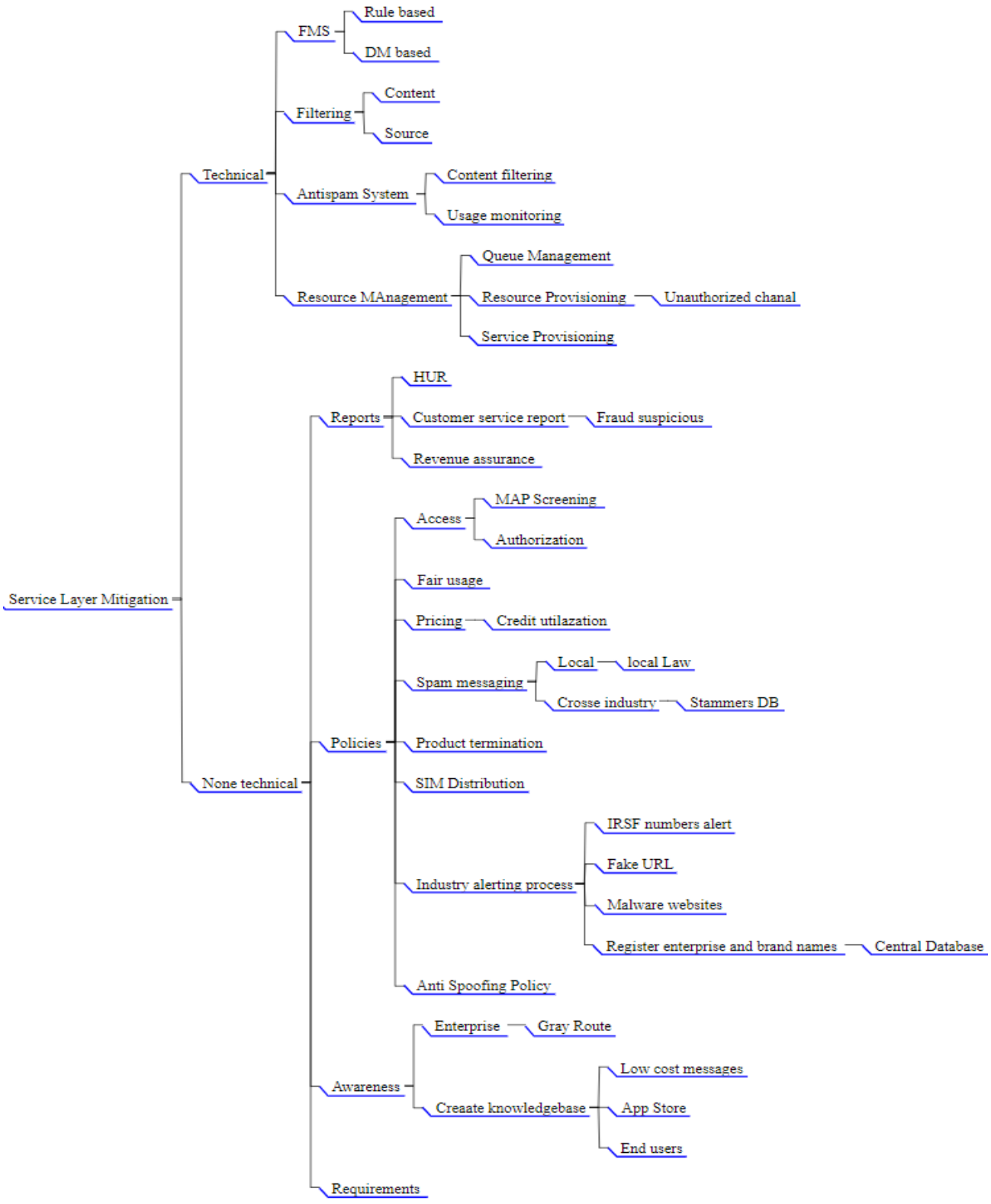
Appendix 2 SMS fraud mitigation taxonomy Mind-map design Vulnerability node



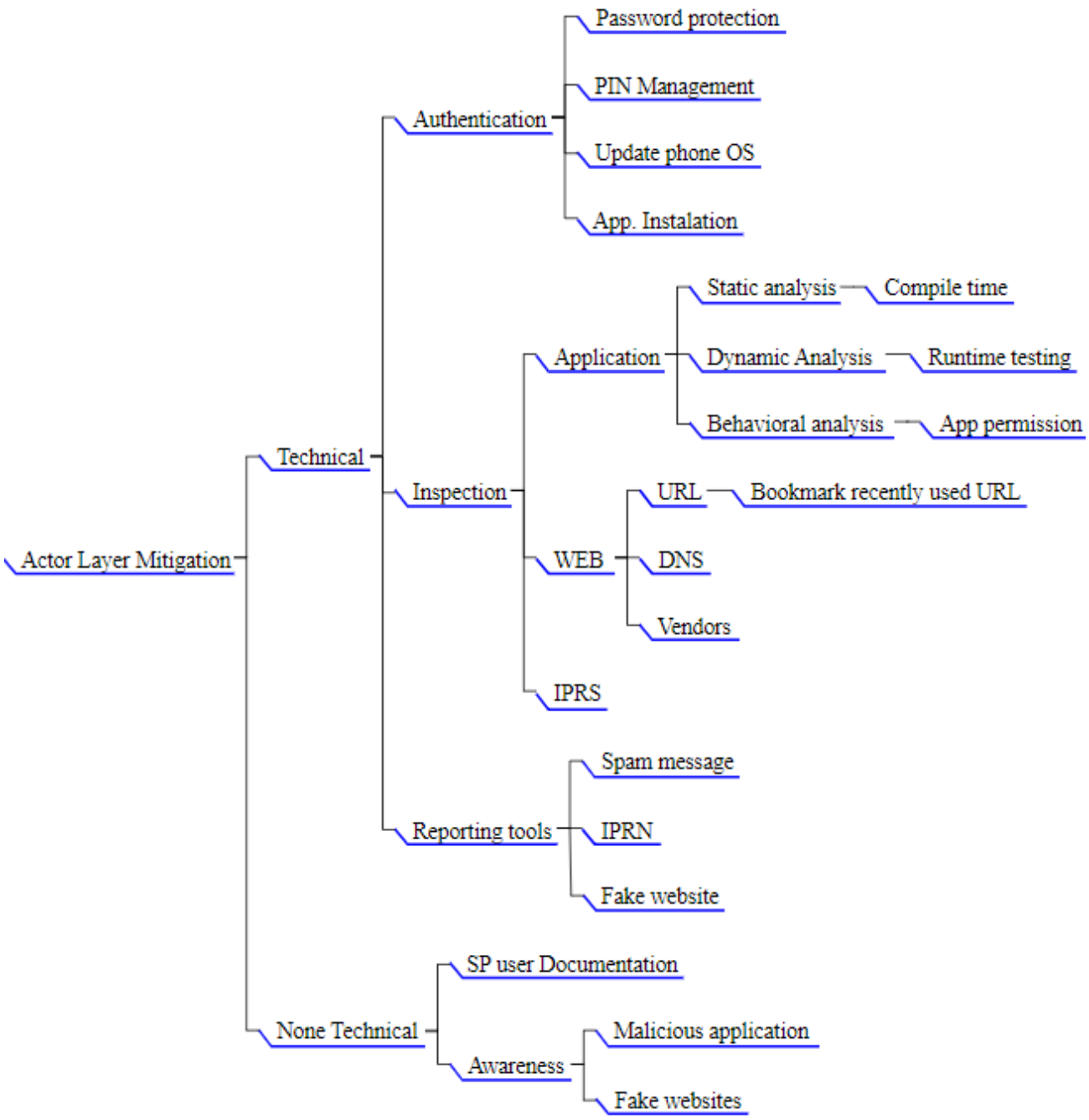
Appendix 3 SMS fraud mitigation taxonomy Mind-map design Network/Protocol node



Appendix 4 SMS fraud mitigation taxonomy Mind-map design Service node



Appendix 5 SMS fraud mitigation taxonomy Mind-map design Actor node



Appendix 6 SMS fraud mitigation techniques Network/Protocol level

To represent the mitigation techniques which are applied to specific fraud type, number 1 and 0 are used as indicator. Number one (1) indicated that the mitigation technique is applicable, Number Zero (0) indicated that the mitigation technique is not applicable. This legend is working for Appendixes 3,4 and 5

1= Applicable

0= Not applicable

		SMS Bypass	GT Faking	SMS Spam	SMS Malware	SMS Hacking
Network/Protocol Technical Mitigation	Apply filters on suspicious traffic [54]	1	1	1	0	0
	Identifying official routes to establish a commercial agreement or to close them [54]	1	0	1	0	0
	Firewalls and routers within mobile operator networks [43]	1	1	0	0	0
	Real time monitoring tool at the international signaling gateway [43]	1	1	0	0	0
	Test Call Generation (TCG) from known application [43, 54]	1	0	1	1	0
	Test traffic generated manually through direct interaction with an application [43]	1	0	0	0	1
	Monitor capricious loads on the network due to bulk SMS [23]	1	1	1	0	0
	Conventional SS7 signaling surveillance systems [23]	1	1	0	0	0
	Monitoring SMSC Global Title, or A_MSISDN is wrong [24]	1	1	0	0	0
	SS7 routing check when SCCP or MAP addresses are manipulated [24, 26]	0	1	0	0	0
	Secure a mobile operator's SMSC at the Message Transfer Part (MTP) level, the signaling point code [5]	1	1	0	0	0
	No alphanumeric support on networks [5,24]	1	1	0	0	0
	Set SCCP alarms or reports, to check calling party Global Title and Service Centre addresses match [5]	0	1	0	0	0
	Enough security precautions to prevent the SMSC from being used as a relay [5]	0	1	0	0	0
	Monitor and identify potential malicious nodes [26]	1	1	0	0	1
	Detect suspicious/abnormal traffic from a GT [26].	1	1	0	0	0

	Filter web applications now use text messaging to interact with their customers [9]	0	0	0	1	1
	Spam and malicious content filtering [6]	0	0	1	0	0
	Trigger alarms to indicate increased traffic flows over the network [12]	1	1	1	1	0
	Monitor large number of messages being sent to one or more destinations [24]	1	1	1	1	0
	Filter messages contains a URL that looks valid or is potentially misspelled [5]	1	1	0	0	1
	Determine the true sender of Brand's Canonical Name (CNAME) record in their DNS records [5]	0	0	1	0	1
	Make restriction and approved on Pre-registration of originator, and No-alpha originators allowed [5]	1	1	1	0	1
	Monitor messages not sent by a real mobile but is generated from a specific system with a C7 application [24]	1	1	1	0	1
	Network so not support for "dynamic" alpha-tag originators [5]	1	1	0	0	0
	Secure back-to-back contractual provisioning from a mobile operator down to a brand or enterprise [5]	1	1	1	0	0
	Evaluate illegal use of the HPLMN SMS-C by a third party [24]	0	1	0	0	0
	Permit only long numbers until a customer proves that they are who they say they are [5]	1	1	0	0	0
	To avoid vishing attacks, white listing a trusted entity [58]	0	0	0	1	1
	Blacklists, Whitelists, Machine Learning approaches [19,20]	1	1	1	1	1
	Tracing back the sender to identify whether the display name has been spoofed [16]	1	1	0	0	1
	Monitor SMS MO with a manipulated A-MSISDN is coming into the HPLMN network from a foreign VLR or SCCP address [24]	1	1	0	0	1
	Hot list of phishing URL sites and block access or provide customers with a warning message before providing access [12]	0	0	0	0	1
	Content filtering to look for specific originators [5]	1	1	0	0	1
	Identify the actual and 'grey route' SMS while sending SMS from TCG SIMs using boundless international routes [23]	1	0	0	0	0
	Establish or enhance the incident management capabilities to be able to respond to incidents in the core network domain [29]	1	1	0	0	0

	Perform cross-layer checking on SCCP layer and GT(s) in the MAP layer belong to the same operator [26]	1	1	0	0	0
	Establish and monitor limits per SMSC based on known traffic patterns to identify high usage [12]	1	1	1	1	0
	Monitor if the displayed number of the message is modified [16]	0	1	0	0	0
	Monitor if many messages containing unknown SSNs which indicates a possible scan of the attacked operator's network [26]	1	1	0	0	0
	Monitor If an operator detects a non-standard sequence/order of packets in a certain time from a specific node [26]	1	1	0	0	0
	Detect a possible vishing attack through checking the verification of the display name during runtime [58]	0	0	0	1	1
	Block the possibility inject SMS messages into the messaging network with a 'spoofed' originator IDs [25]	0	0	0	0	1
	Authentication the mobile originated leg of the message transfer [14]	0	1	0	0	1
	A combination of identifying legitimate originators and active monitoring of messaging traffic [5]	0	1	0	0	1
	Integrate specific DNS security protection to prevent server hacking as an IP Security policy [12]	0	0	0	1	1
	Identify the possibility to send SMS message from the internet with the correct headers [25]	1	0	0	0	1
	Evaluate discrepancies between protocol layers [23]	0	1	0	0	1
	Monitor intent delivery of new SMS received/ sent can't be easily intercepted or manipulated [10]	0	0	0	1	1
	GTs monitoring approach to identify potentially compromised traffic from the compromised 'black' nodes or 'white' nodes [26]	0	1	0	0	0
Network/ Protocol None	Log the usage of specific MAP messages, to monitor network quality [29]	1	1	0	0	0
	Do not allows aggregators and application service providers (ASP) to blend direct connections with Grey Routes [5]	1	1	0	0	0
	Educate closure of routes can result in the sudden failure of all messages [5]	1	0	1	0	0
	Protect Data sovereignty and privacy issues [6]	1	1	0	0	0

Plan to respond to newly identified bypass threats through refinement of their security policies [2]	1	0	1	0	0
SS7 SMS Inspection [23]	1	1	1	0	1
Education across the ecosystem SMS fraud techniques [5]	1	1	1	1	1
Security policies at the SS7 level [6]	1	1	1	0	1
Create clear guidance of what is and is not permitted in terms of message manipulation to remove any risk of ambiguity [5]	1	1	0	0	0
Ensure firewalls are correctly configured whether a Service Centre address has been manipulated [5]	1	1	1	0	0
Do not provide the full Global Title when selling SRI' [5]	1	1	1	0	1
Report to the Home PLMN of the originating MSISDN to have service removed [14]	1	1	1	1	1
Communicate if an operator detects the node associated with the GT has been compromised [26]	1	1	0	0	0
Establish a continuous process for assessing and remediating any discovered vulnerability [29]	1	1	1	1	1
Educate customer, the caller ID displayed on the phone screen is not enough to detect vishing attacks [16]	0	1	1	1	1
A combination of identifying legitimate originators and active monitoring of messaging traffic [5]	0	1	0	1	1
Implement concrete contractual back-to-back arrangement with the sending party and the value chain [5]	1	1	1	0	1
Knowledge base: how trick the SMSC by modifying the low-level signaling parameters of the MO message [14]	1	1	0	0	0

Appendix 7 SMS fraud mitigation techniques Service level

		SMS Bypass	GT Faking	SMS Spam	SMS Malware	SMS Hacking
Service Layer Technical Mitigations	Establish a joined-up digital communications strategy within enterprises [5]	1	1	1	0	0
	Protection on Global Titles and point codes from certain regulators [5]	0	1	1	0	0
	Monitoring for breaches and taking enforcement action as necessary [6]	1	1	1	1	0
	Passive detection through call detail record (CDR) analysis [6]	0	1	1	1	1
	Increase controls and checks on who is bulk buying SIM cards via retail channels [5]	1	0	1	0	0
	Counting Bloom Filters combined with blacklist and whitelist to detect SMS grey traffic on the fly and to block them [59, 55]	1	1	0	0	0
	Identify unauthorized access of SMPP gateway or SMSc [2]	0	1	1	0	0
	Establish end-to-end process to unambiguously identify the fraudulent parties [5]	1	1	1	1	0
	Use SMS Hub to deliver traffic and of message manipulation [5]	1	1	1	0	0
	Establish a globally agreed process involving forensic investigators [5]	1	1	0	1	1
	Cross check the request is sent from the same Global Title [5]	0	1	0	0	1
	Crowd-source information from actual users where possible [5]	0	1	1	1	1
	Create and share a global blacklist of companies [5].	1	1	1	0	1
	Provide industry-wide resources monitoring, recording and mitigating malware [5]	0	0	0	1	0
	Static, dynamic and hybrid approaches by intrusion detection system to detect malware [4]	0	0	0	1	0
	Dynamic analysis involves execution of application in isolated environment to track its execution behavior [27]	0	0	0	1	1
	Machine learning algorithms (SVM, naïve Bayesian method) for learning of known malwares and predicting unknown malware [20, 27]	0	0	1	1	0
	Active monitoring of messaging traffic to filter and identifying legitimate originators [5]	1	1	0	0	1
	Advertise enterprises short codes on their web sites [5]	1	1	1	0	1
	Monitor Customer complaints [12]	1	1	1	1	1
	Monitoring both patterns and message volumes [5]	1	1	1	1	1
	Effective data management and service provisioning [5]	1	1	1	1	1

	Register enterprise and brand names and associated short codes and originators (local or global database) [5]	1	1	1	1	1
	Anti-virus [12]	0	0	0	1	1
	Develop and update a black list of blocked senders [12]	1	1	1	0	1
	Deploy SPAM filters to identify repetitive content and volume [12]	0	0	1	1	0
	Keep an updated white list of all allowable SMSCs [12]	1	1	0	0	0
	Monitor latest phishing technique developments and variations on anti-phishing websites [12]	0	0	0	0	1
	Evaluate unauthorized routes causes confusing and volatile market prices [5]	1	1	1	0	0
	Dedicated SMS fraud management system and generate test calls for tracing [2]	1	1	0	0	0
	Detected by comparing the rate or number of messages in a selected message flow to a pre-selected defined average or expected load [14]	1	0	1	1	0
	Monitor unusual patterns of usage of SMS messaging per customer using the fraud management system [12]	0	1	1	1	0
Service Layer None Technical Mitigation	Proper AA19 / AA60 agreement [5]	1	1	0	0	0
	Control market Price-led procurement activities carried out by aggregators and some Over the Top [5]	1	1	0	1	0
	Protect the ability to meet an enterprise's SLAs can be affected [5]	1	1	1	1	1
	Raise enterprise awareness of the causes and risks of Grey Routes [5]	1	1	0	0	0
	Close and migrate bilateral 'sender keeps all' routes to SMS Hubs to monetize traffic without impacting P2P message streams [5]	1	1	0	0	1
	Educate aggregators to do not manipulate messages to be competitive [5]	1	1	1	1	1
	Report any suspicions to the targeted mobile operators as quickly as possible [60]	0	0	1	1	1
	SMS inter-working agreement with the network whose SMSC is faked then once again there could be inter-operator accounting issues [24]	1	1	1	0	0
	Educate enterprises to stress the relationship between cheaper messaging and poor delivery quality [5]	1	1	0	0	0
	Contracts Follow with third party suppliers [7]	0	1	1	0	1
	Tell the ecosystem about these recycled numbers and the ecosystem is obliged to remove these numbers from any opt-in marketing databases [5]	1	1	1	1	0

	Anti-spam policy that prohibits the use of the mobile network for initiating or sending mobile spam [61]	0	0	1	1	1
	Potential penalties for breaching the anti-spam commitments, including possible suspension and/or termination of contracts [7]	0	0	1	0	0
	Work co-operatively with other mobile operators to address spam issues [7]	0	0	1	1	0
	Monitor Fake Player; Made money by sending messages to premium line numbers [13]	0	0	1	1	1
	Register enterprise and brand names and associated short codes and originators [5]	0	0	1	1	1
	Implement a Code of Conduct for A2P platform providers and aggregators [5]	0	1	1	1	1
	Suspicious Messaging processes, asking for Fake contract renewal [5]	0	0	1	1	1
	Inform users about social engineering practice and fake websites [12]	0	0	1	1	1
	Check the billing system if the billing is made from the SMS-C data, the real subscriber will be invoiced. If the Billing is made from the TAP file, no one will be invoiced [24]	1	1	1	1	0
	Log on criminal offence in most jurisdictions [12]	1	1	1	1	1
	Monitor frontline queries: customer questions and complaints [12]	0	0	1	1	1
	Commercial relationships must be established in advance for A2P messages [6]	0	1	1	1	0
	Collect complaints about texts received by the customer from people they don't know [12]	0	0	1	0	1
	Review customer contracts, Terms & Conditions and/or Acceptable Use Policies [7]	1	1	1	0	1

Appendix 8 SMS fraud mitigation techniques Actor level

		SMS Bypass	GT Faking	SMS Spam	SMS Malware	SMS Hacking
Actor level mitigations (Technical)	Permission based analysis of app. [27]	0	0	0	1	1
	Re-configure phone settings [5]	0	0	0	1	0
	Monitor Software's on phones [5]	0	0	0	1	1
	Crowd sourced malware profiling system [10]	0	0	0	1	0
	Use bookmarks for frequently visited websites [20, 5]	0	0	0	0	1
	Monitor an attempt sending Fake message [1,20]	0	0	1	1	1
	Install genuine applications provided by trusted vendors [20]	0	0	0	1	0
	Anti-phishing tool from trusted vendors [20]	0	0	0	0	1
	Block messages unregistered or unauthorized originators [5]	0	0	0	1	1
	Bookmarking for known URL [5]	0	0	0	0	0
	Forwarding the suspected message to a short code [5]	0	0	1	1	1
	Secure a mobile device by a password and other access control methods [62]	0	0	0	1	0
	Monitor and report if any un used bill [13]	0	0	0	1	0
	Black list and remove Malicious app. [4]	0	0	0	1	1
	host-based and cloud-based protection [18]	0	0	1	1	1
	Automatic end-to-end way to validate whether an originator belongs to a brand or not [5 20]	0	0	1	0	1
	Application Developers: can use a unique identifier instead of the IMEI to protect [63]	0	0	0	1	1
	Filter spam messages at device depending on the type of device being used [12].	0	0	1	0	1
Actor level mitigations (None technical)	Educate mobile subscriber do not agrees to become a "mini SIM Farm" [5]	1	0	0	0	0
	Educate mobile subscriber to do not installs an app provided by a rogue third party [5]	0	0	0	1	0
	Educate the user's about security and privacy and consequently the operator's reputation [2]	0	0	0	1	1
	Working with governments and regulators [7]	1	1	1	1	1
	Provide customers with information and resources [7]	0	0	1	1	1
	Educate the authenticity of permission requested by the application [10]	0	0	1	1	1
	Only download apps from trusted app market [17 10]	0	0	0	1	1
	Know app. Send SMS to premium-rate numbers without user consent [13]	0	0	0	1	1
	Smartphone users should implement a good anti-malware framework [17]	0	0	0	1	1

	Educate how Malware software on mobile network adversely affect the user and/or network [14]	0	0	0	1	1
	Educate different forms of malwares, mobile viruses, spyware and so on [14]	0	0	0	0	1
	App Market Administrators: Remove suspicious apps, Kernel [17]	0	0	0	1	1
	List and communicate fraudulent practice by pretending to be a known company [5]	0	0	1	1	1
	Educate users how to entice people to share personal identity [12]	0	0	0	1	1
	Educate users to do not reply for spoofed website, or Faking messages [28]	0	0	1	1	1
	Protect sensitive personal and confidential financial information [5]	0	0	1	1	1
	Educate: the tricks to entering personal information for breaching account [30]	0	0	1	1	1
	Never reply to any suspicious SMSs [56]	0	0	1	1	1
	During application installation, don't give all permission [64]	0	0	0	1	1
	Educate to the fact that smartphones are essentially are vulnerable to cyber-attacks [17].	0	0	1	1	1

Declaration

I declare that this thesis was composed by myself, that the work contained herein is my own except where explicitly stated otherwise in the text, and that this work has not been submitted for any other degree or professional qualification.

Tarikua Worku _____
Name Signature

Place: Addis Ababa

Date of submission: November 19, 2018

This thesis has been submitted for examination with my approval as a university advisor.

Mesfin Kifle (PhD) _____
Advisor's Name Signature