This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

SS7 Vulnerabilities - A Survey & Implementation of Machine Learning Vs Rule Based Filtering for Detection of SS7 Network Attacks

Kaleem Ullah, Imran Rashid, Hammad Afzal, Waseem Iqbal, Yawar Abbas Bangash, Haider Abbas

***Abstract*—The Signalling System No. 7 (SS7) is used in GSM/ UMTS telecommunication technologies for signalling and management of communication. It was designed on the concept of private boundary walled technology having mutual trust between few national/ multinational operators with no inherent security controls in 1970s. Deregulation, expansion, and merger of telecommunication technology with data networks have vanquished the concept of boundary walls hence increasing the number of service providers, entry points, and interfaces to the SS7 network, which made it vulnerable to serious attacks. The SS7 exploits can be used by attackers to intercept messages, track a subscriber's location, tape/ redirect calls, adversely affect disaster relief operations, drain funds of individuals from banks in combination with other methods and send billions of spam messages. This paper provides a comprehensive review of the SS7 attacks with detailed methods to execute attacks, methods to enter the SS7 core network, and recommends safeguards against the SS7 attacks. It also provides a machine learning based framework to detect anomalies in the SS7 network which is compared with rule based filtering. It further presents a conceptual model for the defense of network.**

***Index Terms*—SS7 vulnerabilities, SS7 attacks, tracking mobile subscribers, call interception, SMS interception, SMS fraud, machine learning, rule based filtering.**

I. Introduction

MOBILE telecommunication networks have enjoyed a great popularity from their start due to a number of factors such as low rates, seamless roaming, wide coverage, and portability of cell phones. After the merger of data and voice networks, their popularity increased manifolds. Popularity of social media, user friendly cell phone applications, enhanced processing power, and memory of cell phones are making this technology even more popular. With the passage of time, telecommunication technology has become primary means of communication for personal needs, business requirements, and emergency services. In telecommunication networks, signalling system is used to set up, manage, and tear down a call [1][2]. The SS7 is used to provide mobility management, control billing information, generate user security information, support call establishment/ termination and control access/ service authorization [3][4][5]. The SS7 network was designed in 1970s when few national/ multinational telecommunication operators used to provide telecommunication services. These national/ multinational operators had access to core network [1][2]. In this backdrop, no inherent security controls were incorporated in the SS7 core network, and it was designed on the basis of mutual trust between operators [6]. It was assumed that all operators, being national/ multinational corporations, can be trusted thus assuming the SS7 network as a closed trusted network [7][8].

Due to convergence between packet-switched IP networks [9] and circuit-switched telephone networks, this technology has seen enormous popularity, competition, and expansion; generating high demand which allowed new players to enter into the market. It also allowed new technologies and interfaces to be introduced with the legacy SS7 network, thus resulting in increased entry points in core network, and increased number of operators having access to this network.

Till late 90s, the services of telecommunication networks, somehow, remained with national/ multinational corporations throughout the world. De-regulation in US (1996) and Europe (1998) legally allowed smaller companies and Mobile Virtual Network Operators (MVNO) to offer telecommunication services to the customers directly[10]-[12]. Purpose of de-regulation was to expand the network, and to remove restrictions on it. Taxonomy of paper is given in Fig. 1. In the current landscape, some limitations are discussed as under:

A. Limited Research by Academia

Convergence of new technologies and deregulation resulted in realization that the SS7 core network is no more a trusted network, which triggered work on its vulnerabilities and defenses. Even after this realization, the SS7 vulnerabilities and exploits have not been widely published or well-known because of complex cellular networks, intricate protocols, and hidden network interfaces [13]. Therefore, these attacks draw less attention of general public as compared to other vulnerabilities of cellular networks. In addition, following points are considered some of the contributing factors to limit the amount of research by academia:

- No access to the real SS7 network due to privacy and legal issues.
- Non availability of any open source simulator or testbed to simulate these vulnerabilities, provide proof of concept for exploitation, and then implement defenses to bridge these vulnerabilities.
- Less interest of network providers as it did not affect their earnings because of no public perception of threat.

B. Motivation

The SS7 exploits can be used by attackers to intercept messages, track a subscriber's location, tape, and redirect calls. These techniques are available not only to intelligence

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

agencies, but to an average hacker as well [14]. These vulnerabilities threaten individual's privacy and have potential to affect disaster relief operations in form of DoS attacks. Tracking of VIPs/ VVIPs location and draining funds of individuals from banks in combination with other methods are also possible by exploiting these vulnerabilities.

The SS7 is used in GSM [15]/ UMTS [16] telecommunication networks. As telecommunication networks are moving towards new technologies like 4G/LTE [17], which use new protocols like Diameter, the question arises that do we need to put an effort to secure the SS7 network as it will be replaced sooner or later? At start of 2017, more than 4.1 billion subscribers were using SS7 network which makes it 87% of total mobile subscribers throughout the world [7].

In 2013 a product with name of *Skylock* appeared in the market whose brochure read "A real time and independent location finding solution for GSM and UMTS subscribers, which enables operational agencies to retrieve subscriber location information on a global basis through use of SS7 messages" [18]. Another product appeared with the name of *Infiltrator Real Time Tracking System* whose brochure read "An innovative tool for governmental and security organizations that require real-time data about suspect's location and movement" [19].

In April 2016, a public statement regarding vulnerabilities of the SS7 was issued in US, "The applications for this vulnerability are seemingly limitless, from criminals monitoring individual targets to foreign entities conducting economic espionage on American companies to nation states monitoring US government officials. The vulnerability has serious ramifications not only for individual privacy, but also for American innovation, competitiveness and national security. Many innovations in digital security such as multi-factor authentication using text messages may be rendered useless"[20].

Documents revealed by Edward Snowden show that US National Security Agency (NSA) is collecting around 5 billion records per day [21]. Among other methods, exploitation of the SS7 vulnerabilities is considered one of the sources of this bulk data. In 2015, an Italian based spyware seller company "Hacking Team" was hacked, and their data was leaked by the hackers. This data showed that the company was selling spywares to different countries and exploiting vulnerabilities of the SS7 network. Their team received offers from other companies to work on the SS7 exploits with them [22].

A study was conducted by *Positive Technologies* [23] on the security of SS7 networks of various service providers from different parts of the world in 2016. Report of the study was published with following findings [1]:

- All tested SS7 networks successfully compromised. It was concluded that no network was completely safe.
- Subscriber's data leak is possible including location disclosure and SMS interception.
- Larger companies, though relatively securer than smaller companies, cannot guarantee complete security.
- DoS attacks on a single subscriber conducted with 80% success rate.
- Fraud including theft of funds conducted with 67% success rate.

TABLE I
LIST OF ACRONYMS AND CORRESPONDING DEFINITIONS

Acronym	Definition
2/3/4G	2nd/ 3rd/ 4th Generation
3GPP	3rd Generation Partnership Project
AIMSICD	Android IMSI Catcher Detector
AT&T	American Telephone & Telegraph
ATI	Any Time Interrogation
AuC	Authentication Center
BSC	Base Station Controller
BTS	Base Transceiver Station
CA	Certifying Authority
CAP	CAMEL Application Part
CAMEL	Customized Application for Mobile Networks Enhanced Logic
CAS	Channel Associated Signalling
CCIS	Common Channel Inter Office Signalling
CCITT	International Telegraph and Telephone Consultative Committee
CCS	Common Channel Signalliing
COO	Change Over Order
EIR	Equipment Identity Register
GMLC	Gateway Mobile Location Centre
GSM	Global System for Mobile
gsmSCF	GSM Service Control Function
GT	Global Title
HLR	Home Location Register
IAM	Initial Address Message
IDP	Initial Detection Point
IDDD	International Direct Distance Dialling
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IMEI	International Mobile Equipment Identity
INAP	Intelligent Network Application Part
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU-T	International Telecommunication Union - Telecommunication
LBS	Location Based Services
LTE	Long Term Evolution
MSC	Mobile Switching Center
MSRN	Mobile Station Roaming Number
MSISDN	Mobile Subscriber ISDN
MTP	Message Transfer Part
MVNO	Mobile Virtual Network Operator
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PRN	Provide Roaming Number
PSI	Provide Subscriber Information
SCP	Service Control Point
SCCP	Signalling Connection and Control Part
SGSN	Serving GPRS Support Node
SIGTRAN	Signalling Transport
SIM	Subscriber Identity Module
SMS	Short Message Service
SMSC	Short Message Service Centre
SMLC	Serving Mobile Location center
SP	Signalling Point
SRI	Send Routing Information for Short Message
SS7	Signalling System No.7
SSP	Service Switching Point
STP	Service Transfer Point
TCAP	Transaction Capabilities Application Part
TMSI	Temporary Mobile Subscriber Identity
TFP	Transfer Prohibited
TUP	Telephone User Part
UMTS	Universal Mobile Telecommunication System
USSD	Unstructured Supplementary Service Data
VLR	Visitor Location Register
VPN	Virtual Private Network

Further media reports showed the possibility of attacks through the SS7 network [24]-[27]. These reports highlighted the issue

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

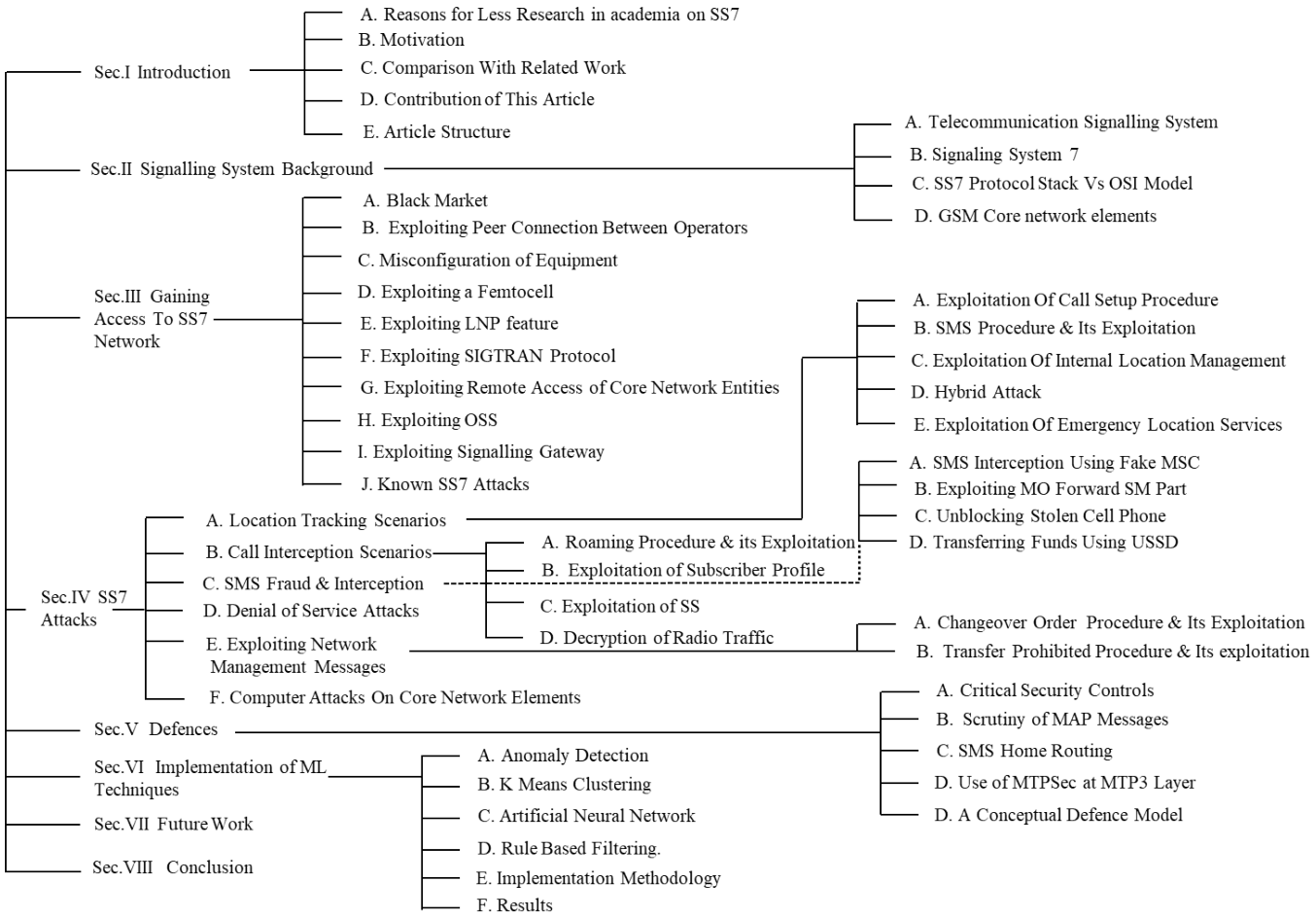


Fig. 1. Taxonomy of the paper.

and raised public awareness about vulnerabilities; due to which it got more attention. There is a dire need to conduct further research and focus on this topic to protect the privacy of the users and ensure safety of individuals. It has become equally important for network operators as fraudulent activities can help the attackers in exploitation of charges in different services.

C. Comparison with Related Work

Most of the literature available on the topic is in the form of formal talks and demonstrations at various forums by telecommunication security specialists from industry. Publication of research papers on the topic remained low as compared to the importance of the topic. No detailed survey paper on the topic is available (to the best of our knowledge) in the literature. Moreover all the published papers either discuss attacks due to application layer protocol or MTP3 layer protocol. This paper combines all possible attacks discussed in papers, dissertations and formal talks on both layers, entry points into the SS7 network and defenses. Moreover, this paper provides implementation of machine learning concepts and comparison of the results with rule based filtering to draw meaningful conclusions. Acronyms used in the paper are given in Table I and summary of related work is given in Table II.

D. Contribution Of This Paper

This paper focuses on providing a comprehensive survey on entry points, attacks, and defenses of the SS7 network. The paper presents following salient points:

- A brief note on the background and evolution of telecommunication signalling systems.
- An overview of the SS7 protocol stack and GSM core network elements.
- Possible entry points into the SS7 network.
- All publicly disclosed location tracking attacks with the detailed method to accomplish these attacks.
- Call and SMS interception, modification and fraud scenarios and attack vectors.
- Possibility of DoS attacks.
- Detailed defenses against the SS7 attacks.
- A machine learning based framework to detect anomalies in the SS7 network which is compared with rule based filtering.
- A conceptual defense model on the basis of an existing model.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

TABLE II: Summary of related work

Reference	Year	Summary
G.Lorenz et al[5][28]	2001	- They explained that attack vectors were increasing due to technological advancements, as the SS7 backbone is merging with internet and wireless communication technologies. - They presented an attack taxonomy. - They highlighted that if an attacker gained access to the SS7 core network, she could change/ delete various databases and customer's record stored in the SS7 core network. - They also highlighted the possibility of SS7 packet sniffing and spoofing due to lack of authentication in SS7 network.
Xenakis et al [29]	2002	- They described an overview of UMTS security covering following aspects: - Network access security mechanism. - Network domain security mechanism. - Provision of User domain security. - Availability of Application security. - Mechanism for Visibility of security. - They presented a brief description of MAPSec. This paper shows that MAPSec ensures transport security of MAP layer and also provides management procedure. It also describes services provided by MAPSec.
H. Sengar et al[2][30]	2005, 2006	- They described the effects of exploiting network management messages (Changeover Order message and Transfer Prohibited message discussed in [2]). - Various signalling links can be declared unavailable and traffic can be diverted away from these links. This can cause: - DoS for a particular destination - Congestion of the network by routing all the traffic through a single link. - Interception by routing traffic through a particular node under control of attacker and a decrease in efficiency by routing all the traffic from farthest possible route.
H. Sengar et al[32]	2006	- They focused on interconnection of the SS7 and IP protocols highlighting, issues and security features due to interconnections. - They highlighted vulnerabilities generated by SIGTRAN protocol and proposed solution to overcome these vulnerabilities in the form access control, screening of incoming/ outgoing signal messages and use of anomaly detection techniques [33].
Philippe Langlois[34]	2007	- P. Langlois (Telcom Security Task Force) delivered a talk in BlackHat Convention (BH) [35], 2007. The talk was focused on finding entry points and gaining access to the SS7 core network. - It focused on vulnerabilities generated due to merger of SS7 and IP networks. - It highlighted that SCTP is vulnerable to simple attacks.
Tobias Engel[36]	2008	A security expert, Tobias Engel, from Berlin-based security corporation Sternraute showed that location disclosure and sending of spam messages was possible with access to the SS7 network.
Kotapati, Kameswari [37] [38]	2008 2009	- The authors developed a toolkit with the name of Cellular Network Vulnerability Assessment Toolkit for Evaluation (eCAT). - They used this toolkit for evaluation of MAPSec to ascertain the security provided by MAPSec. - The authors concluded that MAPSec provides protection against a limited set of attacks. It did not effectively block the most important attacks resulting due to corrupt data sources, and service logic.
Lingling, Jiang and Ma Hong [39]	2009	They discussed effects of exploiting Changeover Order (COO) network management message at MTP3 layer and Initial Address Message (IAM) at application layer.
An Xinyuan et al[40]	2011	They described exploitation of network management messages with focus on presenting a solution to identify counterfeit messages.
Joe-Kai et al[41]	2012	- They presented security analysis of Authentication and Key Agreement protocols of UMTS and LTE. - The key secrecy and entity authentication, based on carrying protocols within the core network investigated computationally. - They conclude that due to no integrity protection in session identifiers, UMTS AKA can be vulnerable when it is running over MAP and MAPsec.
P-Olivier & A-De Oliveira [42]	2014	P1 security experts presented a talk in Hackito Ergo Summit [43] (2014) in which they explained/ demonstrated tracking of the user location and sending spoofed messages.
Karsten Nohl [44]	2014	In Chaos Communication congress [45] 2014, Kristen Nohal from Security Research Labs showed that interception of phone calls and messages is possible with access to the SS7 network.
Tobias Engel [46]	2014	In Chaos Communication congress 2014, Tobias Engel showed the possibility of location tracking and denial of service attacks with access to SS7 network in a live demo. Moreover several other attacks were also explained.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

TABLE II: Summary of related work-continued

Positive technologies [14]	2014	- In December 2014 Positive technologies issued a white paper based on research conducted by their experts which concluded that several attacks were possible if an attacker has access to the SS7 network. - They also offered their products PT the SS7 scanner and PT IDS-SS7 to help overcome these vulnerabilities.
S.P Rao et al [13]	2015	- They presented an overview of the SS7 location disclosure attacks with details of methods to accomplish attacks. - A brief report on entry points of SS7. - They suggested a generic approach and recommended good practices to safeguard the network from a possible attack.
SP Rao [47]	2015	- They described details of all SS7 attacks, mainly due to exploitation of MAP messages. - They explained the method of completing each attack.
Hassan Mourad [8]	2015	SANS institute published a white paper which provided an overview of possible attacks on the SS7 network and suggested some of critical security controls to be used for better protection of the SS7 network.
D-Kurbatov & V-Kropotov [4]	2015	Positive Security experts, D. Kurbatov and V. Kropotov presented a talk in 2015 explaining entry points of the SS7 and few attack scenarios were explained/ demonstrated.
Kristoffer Jensen[48] [49][50]	2016, 2017	- They presented a brief overview of the SS7 attacks. - They outlined a short note on methods to enter into the SS7 core network. - They focused on the use of machine learning algorithms to detect attacks on the SS7 network. - They presented a simulated prototype to detect attacks using one type of MAP messages through machine learning techniques. - They introduced an open source simulator with the name of "SS7 Attack Simulator" [51] to produce simulated SS7 normal and attack traffic.
S. Holtmanns et al[52]	2016	- They described that the SS7 vulnerabilities threaten LTE users as well in addition to GSM/UMTS users. - These vulnerabilities can be exploited to track LTE users using Diameter protocol because of interworking functionality [53]. - These attacks work on certain assumptions like no IPSec is used between interworking nodes, IP address filtering is not used, receiving node performs no sanity check, attacker knows Mobile Station International Subscriber Directory Number (MSISDN) of victim and address of edge node.
M. Savadatti and D. Sharma [54]	2017	- They gave an overview of the signalling system No.7 and outlined a short description of the SS7 attacks without any details of methods to accomplish these attacks.
S. Puzankov [55]	2017	- They discussed stealthy attacks resulting due to SS7 vulnerabilities. - Suggested that SMS home routing could be bypassed due to misconfiguration errors which could result in IMSI disclosure of the subscriber to launch further sophisticated attacks. - Stealthy location tracking attack can be accomplished by silent USSD notification instead of silent SMS, as silent SMS is stored in user account whereas silent USSD notification is not stored in user account. - Interception of short messages can be done in a stealthy manner and for a longer period. - An attacker can register the subscriber in a network using fake MSC while VLR remains the legitimate one. In this case legitimate MSC will be used for voice calls and originating short messages while fake MSC will be used to intercept incoming messages.
Nathanael Andrews [56]	2018	- The Author discussed SIM-Swap attacks. - The SS7 vulnerabilities can be exploited to compromise SMS system to intercept text messages of a user.
Liu C X, Ji X S, Wu J X, et al. [57]	2018	- They discussed compromise of user identities, location, and security parameters due to vulnerabilities of the SS7 network. - They proposed a defense model to secure user data
Abdelrazek, Loay, and Marianne A. Azer. [58]	2018	- They discussed location tracking and interception of calls/SMS due to vulnerabilities of the SS7.
Qasim, Tooba, M. Hanif Durad, et al. [59]	2018	They discussed the SS7 vulnerabilities in in following four categories: - Compromise of user information such as IMSI and possibility of location tracking. - Possibility of eavesdropping on incoming and outgoing calls - Possibility of Financial thievery (exploitation of USSD) - Possibility of Misuse of service (exploitation of user billing)
Aung, Tun Myat, et al. [60]	2019	- They discussed vulnerabilities in SMS sending/ receiving procedure. - They stated that SMS services are used to send important information from one user to another user. SMS services can be exploited and data can be intercepted.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

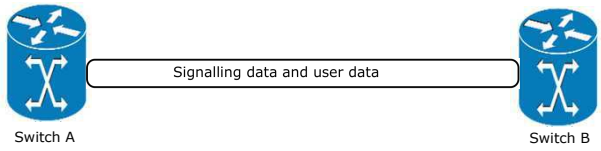


Fig. 2. Channel Associated Signalling.

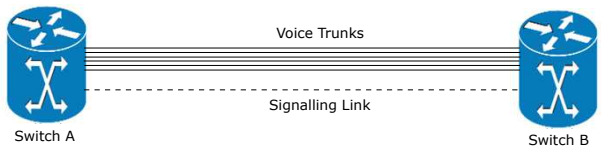


Fig. 3. Common Channel Signalling (associated mode)[61]

.

E. Article Structure

The rest of the paper is organized as follows: Section II presents an overview of the SS7 protocol stack and GSM core network elements; section III explains possible ways to enter the SS7 core network and summarizes known SS7 attacks; section IV discusses SS7 attacks including location tracking cases, call interception scenarios, SMS fraud and interception cases, DoS attacks, exploitation of network management messages, and computer attacks on core network elements; section V underlines the defenses against SS7 attacks; section VI provides implementation of machine learning concepts and comparison with rule based filtering; section VII proposes future work; section VIII concludes the paper.

II. SIGNALLING SYSTEM

A. Telecommunication Signalling System

Telecommunication networks utilize signalling system for establishment, management, and release of calls. [62]. Signalling system can be called as command and control system of the telecommunication networks; which enables two subscribers to connect with each other. It enables seamless handover when one subscriber is on the move, assists in location tracking of the subscribers for the purpose of routing calls directly to correct location, and provides various other supporting functions and features. In GSM/ UMTS, the SS7 network is used to provide all above functions.

1) Channel Associated Signalling (CAS): In this type of signalling, same channel is used for transferring control information (signalling) and actual traffic of the user (voice, data) [63] as shown in Fig. 2. As control information is being sent in the same band which is being used for actual data of the user, it is called in-band signalling. Examples of CAS include Signalling System no 5 (SS5) which was used before 1970. Disadvantages of CAS/ SS5 are as follows:

- It was inefficient as signalling and actual subscriber's data was competing for transmission.
- Less bandwidth was available to carry subscriber's data as signalling messages were consuming part of the bandwidth.
- It required additional signalling equipment at every node to forward signalling data.
- Resources of the channel were reserved as soon as signalling started. Even if the recipient was busy or unavailable, the channel remained occupied.
- Subscribers were able to access signalling messages creating possibility of malicious activities by the subscribers. Due to these disadvantages CAS was replaced with Common Channel Signalling (CCS).

2) Common Channel Signalling: In CCS, signalling messages are passed on a separate logical path than subscriber's data. It is called common channel signalling because this channel is used commonly to accommodate signalling data of all calls. All signals related to call initiation, management and termination are passed on this channel independent of subscriber's data. The SS6 and the SS7 are examples of CCS [62]. An illustration of CCS is shown in Fig. 3 Advantages of CCS are as follows:

- This signalling system is very efficient as it reduces time to set up a call because of dedicated signalling channel for signalling messages.
- Signalling and calling can simultaneously be performed without competition as both have separate paths.
- It is more reliable as compared to Channel Associated signalling as it provides opportunity to achieve redundancy in signalling.
- Subscribers cannot directly access signalling data as the end users, thus eliminating chances of any malicious activity by subscribers.

B. Signalling System No 7

In 1970s, the use of SS6 and CCIS was only limited to international and American Telephone & Telegraph (AT&T) networks [64]. A new system was developed by Consultative Committee International Telephone and Telegraph (CCITT) which was initially known as CCITT 7 with the aim of developing a system capable of being used worldwide as a standard. The initial development of the system was for the control of calls only. The standard was published in CCITT yellow book of 1981. Since then, it has undergone numerous updates and modifications from time to time, and now it is called SS7 . In this paper, its functionality has been defined and its components, which are essentially required for the scope of this paper, has been briefly described. The SS7 was primarily developed for initiating and terminating a call but with the technological advancements, its functions have evolved and it includes following tasks now:

- It enables communication between core network entities for routing of calls.
- It supports seamless handover of call from one MSC to another MSC when subscriber is moving.
- It provides roaming facility.
- It is used to generate billing information.
- It provides Short Message Service (SMS) initiation and delivery.
- It provides location tracking facility for emergency services.
- It provides toll free (0800) services for government and private organizations [65].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

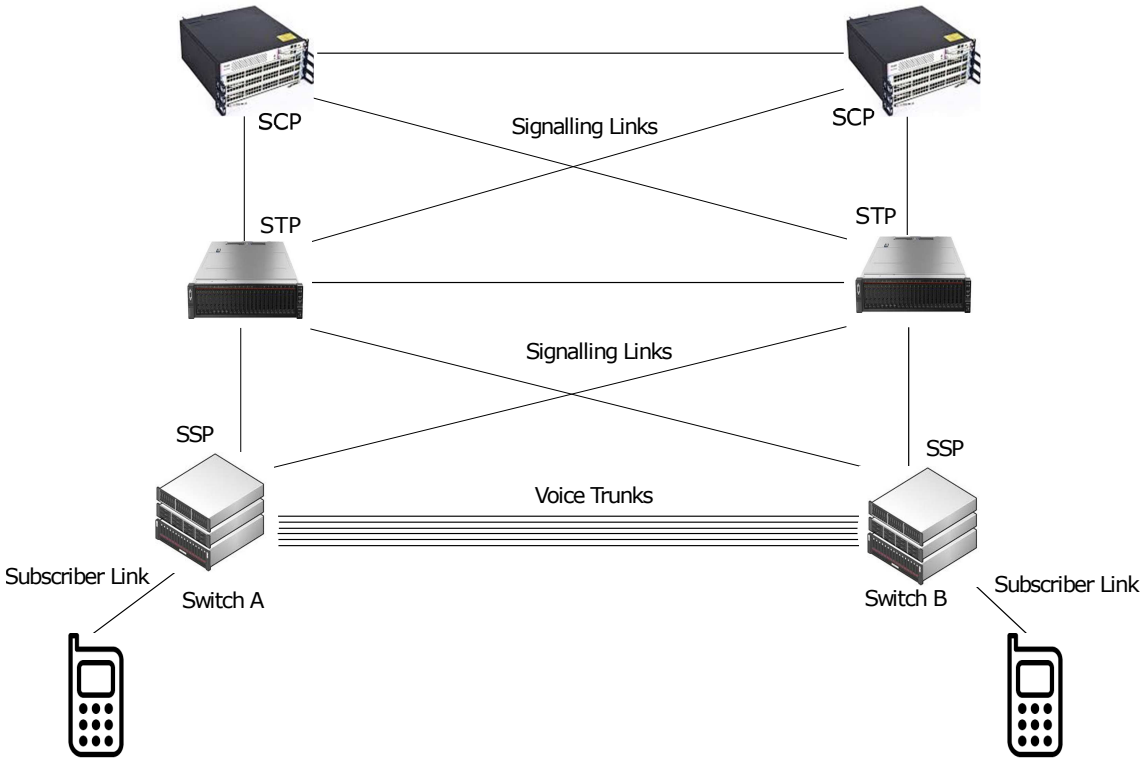


Fig. 4. Basic Building Blocks of the SS7 Core Network [65]

- It provides additional services like call forwarding and display of calling number.

Few basic elements of the SS7 are described as under:

1) Subscriber Link: It is used to carry data of the subscribers from end device (phone) to the switch.

2) Signalling Links: They are used to carry signalling data between different nodes of the SS7 for signalling purposes. In the SS7 network dedicated and out of band links are used for signalling purpose as shown in Fig. 4 [66].

3) Voice Trunks: They are used to carry voice data of the user after call has been established.

4) Service Switching Point (SSP): The SS7 network consists of three basic signalling points for management of signalling. These signalling points are connected through signalling links as shown in Fig. 4. Primary function of an SSP is to initiate a call when the user dials a number and to terminate a call upon completion. It also gives dialling tone, converts dialled number to the desired code of switch to which it has to be forwarded, and communicates with STPs and SCPs [65]

5) Signal Transfer Point (STP): Primary function of an STP is to perform routing of incoming signals from SSPs. SSPs forward all signals to STPs which further route them to the destination. All SSPs do not require direct connection in the presence of STPs [65].

6) Signal Control Points (SCPs): SCPs insert intelligence into the SS7 network and provide extra features. It gives instructions to SSPs on how to route calls. Whether to forward the call or not. It runs Customized Application for Mobile Networks Enhanced Logic (CAMEL) [67] services as well [46].

7) Future of SS7 Signalling Network: Telecommunication operators are moving towards 5G, after success of 4G, but there is a huge difference of time exists around the world between different regions in adoption of new technologies and obsolesce of old technologies. Till the time, all mobile operators do not shift from 2G/3G to 4G/5G, use of the SS7 will remain there. 4G/5G mobile operators will be providing backward compatibility in order to ensure worldwide coverage/ roaming facility. As per white paper at [68], by 2020, more than 60% of the mobile subscribers in South Asia, more than 40% of the users in Africa and more than 50% of users in Western Asia & Eastern Europe will be using 2G networks. The SS7 is expected to remain in service for many years to come.

C. SS7 Protocol Stack Vs OSI Model

For better understanding of the SS7 layers and their functionality, a comparison of this stack with well known OSI model is shown in Fig. 5[69].

1) Message Transfer Part (MTP): MTP-1 is the lowest level at the bottom of the stack. It is analogical to physical layer in OSI model. It defines physical characteristics like voltage levels and physical connections. MTP2 is the next layer and is analogical to data link layer in OSI model. It ensures accuracy of message transmission and delivery from end to end. It also ensures flow control, keeps a check on errors, and responds with the retransmission in case of an error. MTP3 decides routing path of the signals. It keeps state of all nodes and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

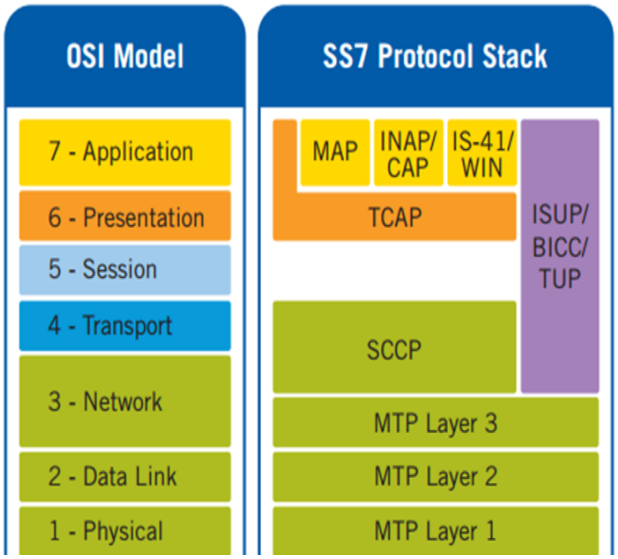


Fig. 5. A Comparison of SS7 protocol stack vs OSI protocol stack [70]

routes in the network and re-routes traffic from a different path in case of failure of a particular node. It also carries out congestion control of the network [65]. It is analogical to network layer in OSI model.

2) Signalling Connection Control Part (SCCP): SCCP provides network services and enhanced routing features. Every SP has a physical address in the SS7 network which is called Global Title (GT). SCCP provides functionality of global title translation. It translates GT of the destination into a format which identifies destination SP and destination application. In combination with TCAP services, it can be considered analogical to transport layer of OSI model.

3) Telephone User Part (TUP) & ISDN User Part (ISUP): ISUP enables network connections (e.g., call setup, release). It provides services associated with call set up and termination[71]. It contains following types of messages:

- Initial address message (IAM)
- Subsequent address message (SAM)
- Address complete message (ACM)
- Call progress (CPG)
- Answer message (ANM)
- Connect (CON)
- Release (REL)
- Release complete (RLC)

Telephone User Part (TUP) was designed to provide PSTN telephony services. Though it was designed to provide services for all applications, but its fundamental telephony-based networks design limits its efficacy. It is being replaced by ISUP.

4) Transaction Capabilities Application Part (TCAP: It enables communication between SPs within a network. MAP and CAP services are provided through TCAP messages. TCAP is used for query and query response messages between SPs within a network. 3GPP has released an extension to TCAP for security of TCAP messages which is called TCAPSec[72]. It has been designed to provide following services:

- Integrity of data.
- Authentication of data origin.
- Anti-replay protection.
- Confidentiality (optional).

5) Mobile Application Part (MAP): The SS7 protocol was initially designed to initiate and terminate a voice call. Later it was modified to include extra features. One of the most important modifications with respect to scope of this paper was introduction of MAP which is an application layer protocol. It was defined by the 3rd Generation Partnership Project (3GPP). Its basic functionalities include seamless handover, mobility management, roaming services, short message, and location services along with many other additional services. It provides 81 different services [73]. The most important entities in the core network like Mobile Switching Centre (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Short Message service centre (SMSC) and Equipment Identity Register (EIR) use MAP messages to ensure above mentioned services. The idea behind development of MAP is to allow communication between different data bases and switching centres for coordination and location management.

3GPP has released an extension of MAP protocol for security at application layer[75]. It also mandates use of MAPSec at network layer in case of IP is being used as a transport layer.

It has three modes

- Protection mode 0-No protection.
- Protection Mode 1-Integrity Protection
- Protection Mode 2-Confidentiality and Integrity protection

6) CAMEL Application Part (CAP): CAP provides an additional set of features through CAMEL to the network providers[67].

D. GSM Core Network Elements

Some of the important core network elements are shown in Fig. 6

1) Mobile Switching Centre: MSC is an interface between radio and the fixed network of a service provider. Basic functions of MSC include routing of calls, short messages, and to ensure seamless handover of calls with other MSCs. If an MSC has the ability to forward calls and messages to the MSCs of other networks, it is called gateway MSC (GMSC) [76].

2) Home Location Register (HLR): It is part of the master database Home Subscriber server (HSS) of any network operator. Home Location Register stores position information about a subscriber so that calls can be forwarded directly to the required subscriber. It also contains subscription profile information of a subscriber which includes call forwarding requests and services user allowed to access[46][78]. For anonymity and security, International Mobile Subscriber Identity (IMSI) is used rather than Mobile Station International Subscriber Directory Number (MSISDN). This mapping is maintained in HLR in the network [13].

3) Authentication Centre (AuC): Its function is to authenticate a user before giving permission to access the network. It stores the pre shared cryptographic keys and identities of the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

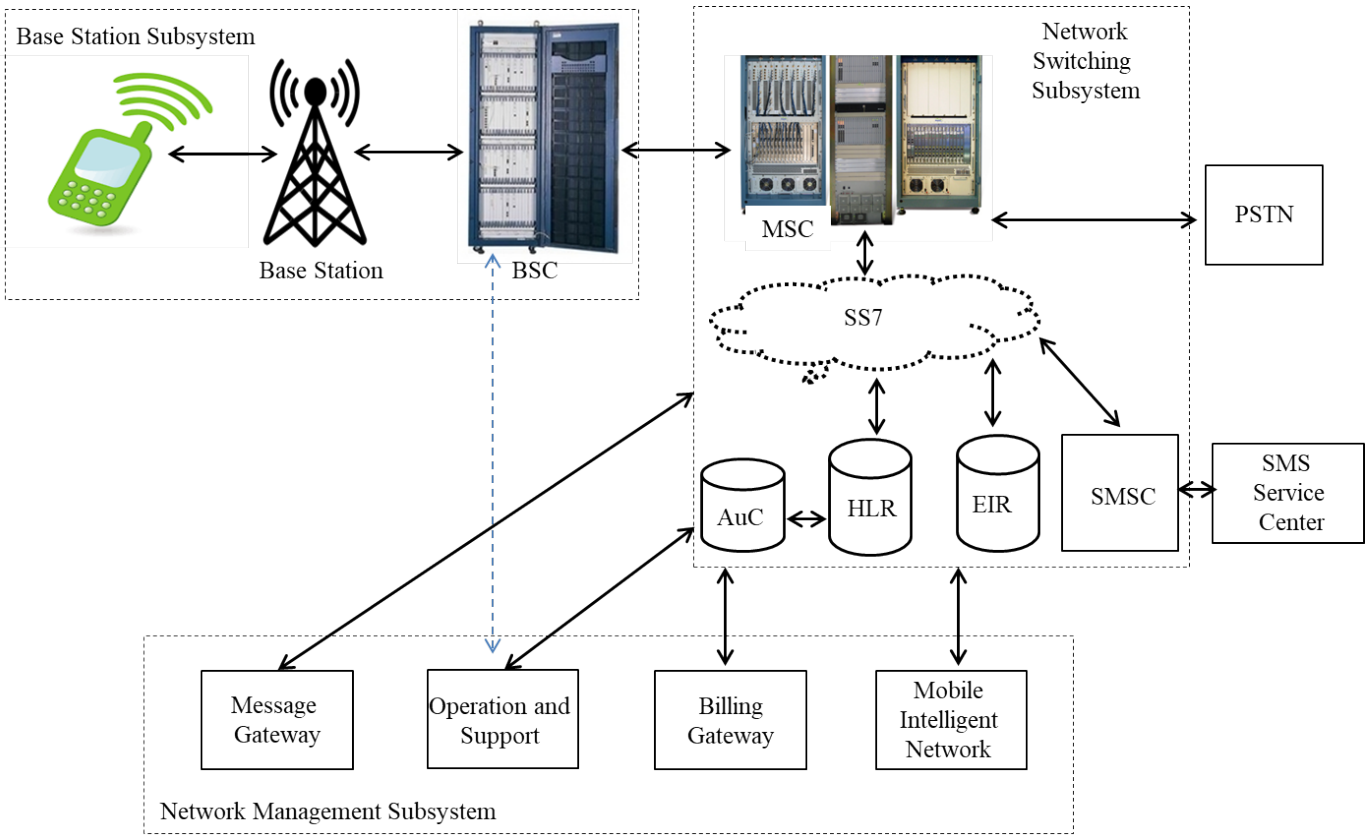


Fig. 6. GSM core network subsystems, elements, databases, and components which are responsible to connect the two users [77].

users. It also generates session keys to be used for encryption of traffic in a session.

4) Visitor Location Register (VLR): There is one VLR with each MSC. All the data about the subscriber is initially stored in HLR. A copy of the subscriber's data is forwarded to VLR by HLR for all subscribers which are being served by a particular MSC so that MSC is not required to query the HLR for details about the subscriber every time subscriber invokes a service rather the details should be available with VLR [76].

5) Equipment Identity Register (EIR): Each cell phone is uniquely identified by International Mobile Station Equipment Identity (IMEI). This is analogical to MAC address in a computer. EIR stores IMEIs of all cell phones which are allowed to access the network (White List), which has been blocked and are not allowed to access the network (Black List) and which can access the network with a condition that they can be tracked for security purposes (Grey List). These lists are used to ensure that a stolen cell phone is not able to access the network [76].

6) Short message service centre (SMSC): SMSC is used to route short messages directly to the desired MSC or SMSC. It communicates with HLR to fetch the whereabouts of the user and forwards the message directly to the serving MSC without sending it to HLR or home MSC [79]. It also stores the incoming messages, then forwards them to the destination [80].

7) Identifiers Used in the Core Network: Various terminologies and identifiers are used as defined by 3GPP in the core network to identify a user and equipment. Each cell phone is uniquely identified by IMEI [81]. International Mobile Subscriber Identification (IMSI) is a 15 digit number which is used to identify a Subscriber Identity Module (SIM). It is the identity of the subscriber and is kept secret. It is used within core network only. It is also used to identify and authenticate a SIM when it access to a network [82]. Mobile Station ISDN (MSISDN) is the number of SIM which is used to call to a particular individual. It is mapped with IMSI and this mapping is maintained in core network[82]. Global Title (GT) is used to identify each element in the network for communication with each other for routing and management of calls [73].

III. GAINING ACCESS TO SS7 NETWORK

Attacks using the SS7 vulnerabilities have been explained in this paper based on assumptions that the attacker possess following capabilities [43]-[45] :

- Access to the SS7 network.
- Ability to map core network entities.
- Ability to impersonate as any entity within the SS7 network.
- Ability to generate and receive messages to and from core network entities
- Ability to store, modify and forward messages and calls.

From above stated assumptions, the most important and difficult is to get access to the SS7 network. Once attacker has gained access to the SS7 core network, rest of the capabilities depend on professional knowledge and skill set of the attacker

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

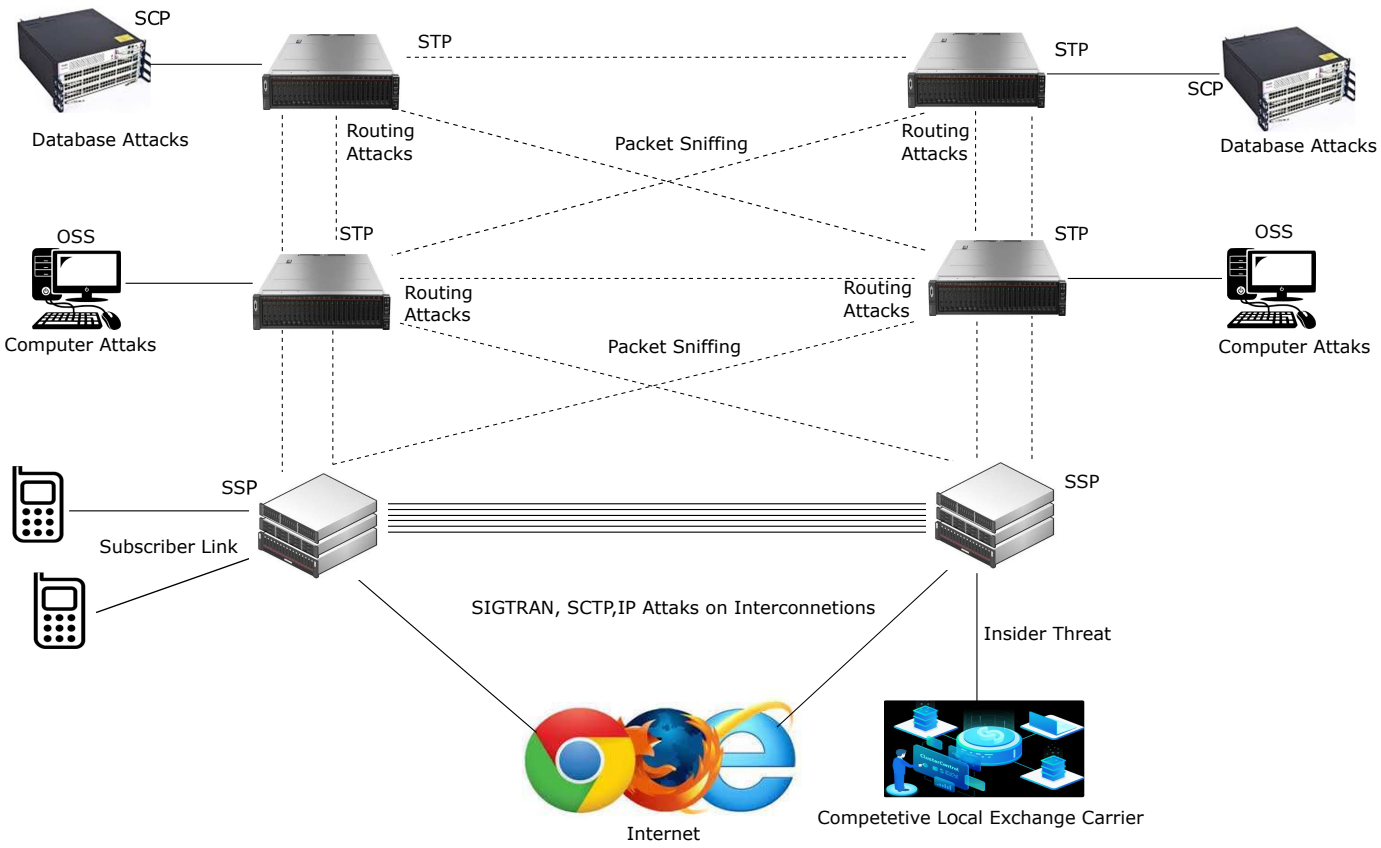


Fig. 7. Attack vectors for entry into the SS7 network [5] - Routing attacks can compromise SCTP, Database attacks against SCP can be materialized, vulnerabilities of SIGTRAN/ SCTP/ IP protocols can be exploited on interconnections of the SS7, and packet sniffing is possible within the SS7 network.

and are not considered difficult. Access to the SS7 network can be obtained by a number of ways. Fig. 7 shows an overview of attack vectors for entry into the SS7 network. Attacker can use open source tools/ programs or can make proprietary tools and softwares to gain capabilities listed above. The SS7 network was defined in 1970s when core network was considered a closed network with access of only few trusted operators. With popularity of telecommunication networks and outspread of internet, the technology broke all walls. Both the technologies (telecommunication and internet) merged, which required modification in the SS7. New interfaces were defined to enable packet switch and circuit switch networks to be merged. This merger has brought together two different industries together i.e telecommunication and IT which resulted in creation of interconnection with vulnerabilities.

Due to increased demand, new / smaller companies entered in competition with national/ multinational companies. With security point of view, bigger companies were having more experience and expertise in field of security. Smaller companies have less expertise and have budget constraints. Hence these are more vulnerable. Due to increased number of operators and interfaces, entry points to the core network have increased manifolds thus threatening the exploitation of the SS7 vulnerabilities.

A number of possible entry points have been published in literature which are summarised in table III. A brief explanation of each attack vector for entry into the SS7 network is discussed in this section.

A. Black Market.

Access to the SS7 may be purchased at black market. A professional hacker or a group of hackers may compromise the SS7 core network and then sell it in the black market [14][48]-[50]. A small company may be established by the malicious users which can cell the SS7 access in black market for financial gain. Moreover, rogue employees having access to the SS7 network can sell the network connectivity in black market for revenge from the company or for financial gain.

B. Exploiting Peer Connection Between Operators.

One of the attracted features of telecommunication networks is worldwide connectivity. With a single sim, a subscriber wants to remain connected with the whole world for personal and business requirements. This feature is ensured through interconnectivity between operators. Quality and coverage area of the network also increase as number of interconnecting operators rise. If an attacker exploits one of the network operators; due to interconnectivity, privacy of all the subscribers of interconnected operators will be at risk [83]. After successful exploitation of one network operator, the attacker will be able to send malicious SS7 messages to other interconnected networks which will endanger privacy of subscribers of all interconnected operators.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

C. Misconfiguration of Equipment.

Due to expansion, competition, and merger of voice and data networks; new protocols and interfaces were defined. New protocols like Signalling Transport (SIGTRAN), Stream Control Transmission protocol (SCTP) [84], and Session Initiation protocols were introduced and merged with the SS7 network. Though this merger created many advantages for the subscribers, it also allowed sending of the SS7 messages over internet. Misconfigured core network entities can be found on internet through which the SS7 network can be accessed [83]. If due to misconfiguration of equipment or mistake of the network manager, the SS7 network elements are accessible over the internet, they can be exploited to gain access to the SS7 network.

D. Exploiting a Femtocell.

A femtocell is a small device to which mobile phones connect. It sends all the data of the user over the internet to the service provider's network [85]. Femtocells have shown insufficient security resistance to attacks. If a service provider has deployed femtocell, it can be exploited by an attacker to get access to the core network[14][83].

E. Exploiting SIGTRAN Protocol.

SIGTRAN [88] protocol was defined as an extension to the SS7 protocol suite to accommodate IP traffic and to enable merger of circuit switched data with packet switched networks. SIGTRAN is one of the gold mines for the attackers with respect to entry into the SS7 [47]. This merger has brought together two different industries together i.e telecommunication and IT. Both industries have different experience, expertise, threat perception, threat exposure, and meaning of threat. It caused troubles in creating standards for merger of both technologies and resulted in vulnerabilities in the interconnection. SGTRAN also gives opportunity to the attacker to learn infrastructure of the core network. It can be used to find out the internal addresses of the core network entities. It uses stream control transmission protocol (SCTP) [89]. There are several techniques available to scan any system for SCTP ports. Tools like SCTPScan [34][83][90] and Scapy [91] can be used for this purpose.

F. Exploiting Remote Access of Core Network Entities.

Core network components can be deployed at various different locations with a centralized control and management system. The management post gets access to the system through company intranet. This remote access gives rise to insider and outsider threats. If the company uses a relatively insecure application for remote access, it can be vulnerable to active attacks and sniffing. Using a default user name and password on these elements will prove a gold mine for the attackers [86]. Remote access of the network is specially vulnerable to insider threat. A disgruntle employee having grudge against the company or having financial greed can be vulnerable in providing access to third parties.

G. Exploiting Operations Support System (OSS).

OSS is normally a set of computers used to perform various management tasks, troubleshoot problems, and to implement new solutions [5]. This system can be vulnerable to well-known computer attacks with the help of Viruses, logic bombs, backdoors, Trojan horses, and worms.

H. Exploiting Signalling Gateway.

Signalling gateway connects nodes which use different protocols i.e., SS7 & IP connection. As signalling gateway is connected to IP network on one side, there are a number of known IP attacks which can be launched to compromise signalling gateways [86]. IP networks have known vulnerabilities which can be exploited. As IP network is connected to the SS7 network, these vulnerabilities become very important in context of the SS7 network.

I. Exploiting Local Number Portability (LNP) Feature.

Local number portability is a service in which a subscriber can change her network provider while keeping the same number [92]. Network providers incorporate LNP feature into their SCPs through some Application Programming Interface (API). These APIs have shown little resistance to attacks, and can be exploited to get desired information and secret identifiers about a user [47].

J. KNOWN SS7 ATTACK TYPES

A number of attacks have been reported by researchers/ security experts. Fig. 8 shows a summary of published attack vectors. In next section, these attacks will be explained in detail.

IV. SS7 Attacks

A. LOCATION TRACKING SCENARIOS

1) Normal Call Setup Procedure: Normal call setup procedure is as under [73][93][94]:

- When a subscriber A dials the number of subscriber B, An Initial Address message (IAM) is sent to MSC via BTS.
- MSC needs to know the address where this call is to be forwarded. It asks HLR about the location of serving MSC with MAP Send Routing Information (SRI) message. HLR acknowledges this message with GT of serving MSC and associated IMSI of the subscriber if subscriber is present within the home network.
- If subscriber is roaming outside home network, HLR has the address of serving MSC in the roaming network but does not have the roaming number (a temporary number allocated to a roaming subscriber by the roaming network). HLR sends MAP Provide Roaming Number (PRN) message to MSC/ VLR in the visited network.
- Visited MSC/ VLR replies with MAP PRN acknowledgement message which contains Mobile Station Roaming Number (MSRN) and associated IMSI of the required subscriber.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

TABLE III
SUMMARY OF POSSIBLE ENTRY POINTS INTO SS7 NETWORK

Reference	Possible Entry Point
Kristoffer Jensen[48], P. Langlois [83]	**Exploitation of interconnectivity between Mobile network operators** Most of the network operators in the world are interconnected with each other. If network of one network provider is compromised, attacker can exploit interconnectivity between operators to get into network of other operators
D-Kurbatov & V-Kropotov [4], Kristoffer Jensen[48][49][50]	**Exploitation of misconfigured equipment** Protocols like Signalling Transport (SIGTRAN), Stream Control Transmission protocol (SCTP), and Session Initiation protocols have been merged with SS7 network for sending SS7 messages over internet. Misconfigured core network entities can be found on internet through which SS7 network can be accessed.
D-Kurbatov & V-Kropotov [4], Positive technologies [14], Tobias Engel [46], SP Rao [47], Kristoffer Jensen[48], S. Puzankov [55] P. Langlois [83]	**Hacking a Femto cell/ edge device** Femtocell sends all the data of the user over the internet to the service provider's network . If a service provider has deployed femtocell, it can be exploited by an attacker to get access to the core network.
Philippe Langlois[34], Kristoffer Jensen[48],P. Langlois [83], T. Moore, T. Kosloff et al [86], Yeboah, Paul Ntim [87]	**Attacking SIGTRAN/SCTP protocol/ signalling gateway** Signalling gateway connects nodes which use different protocols i.e., SS7 & IP connection. As signalling gateway is connected to IP network on one side, there are a number of known IP attacks which can be launched to compromise signalling gateways. SIGTRAN gives opportunity to the attacker to learn infrastructure of the core network and can be used to find out the internal addresses of the core network entities.
Positive technologies [14], Kristoffer Jensen[48]-[50], S. Puzankov [55]	**Purchasing illegal access from black market** Access to SS7 can be purchased at black market from a professional hacker or a group of hackers.
D-Kurbatov & V-Kropotov [4], S. Puzankov [55]	**Getting legal access with a license** Legal access to SS7 network can be bought from a service provider with malicious intent.
SP Rao [47]	**Exploitation of ISDN (ISUP) messages** ISDN (ISUP) messages can be exploited to get access to SSP. Moreover, overloading SSP by sending traffic more than its capacity can also be done to create a DoS attack for that SSP.
Tobias Engel [46]	**Finding unsecured telecommunication network elements on the internet** Unsecured telecommunication network elements can be found over internet due to negligence/ lack of knowledge of network manager.
D-Kurbatov & V-Kropotov [4], T. Moore, T. Kosloff et al [86]	**Insider threat** Through a Access can be obtained through a disgruntle employee of a telecommunication company. Hence, possibility of insider attack can not be over ruled.
T. Moore, T. Kosloff et al [86]	**Exploitation of remote access of core network entities** Remote access of core network elements is vulnerable to insider and outsider threats. If a company uses a relatively insecure application for remote access it can be vulnerable to active attacks and sniffing.
G.Lorenz et al[5]	**Exploiting Operations Support System (OSS)** Operations Support System (OSS) used to perform various management tasks, troubleshoot problems, and to implement new solution. This system can be vulnerable to well-known computer attacks.
SP Rao [47]	**Exploiting Local Number Portability** Local number portability can be exploited to get access to core network

- HLR forwards this message to MSC/ GMSC along with GT of serving MSC/ VLR. MSC/ GMSC routes the incoming call to serving MSC which forwards this call to the recipient.

2) Exploiting Call Setup Procedure for Location Tracking: There are no inherent security controls and authentication mechanism within the SS7 core network. The attacker successfully exploits the above mentioned procedure. she can extract the IMSI associated to the subscriber, GT of MSC, and roaming number in case a subscriber is roaming in other network [36]. This attack, as shown in Fig. 9 is accomplished in following way:

- Attacker knows only MSISDN which is SIM/ cell number we use to dial when making a call. She impersonates as GMSC and sends a message MAP SRI to HLR containing MSISDN of the victim.
- As there is no authentication mechanism in the core network, HLR will forward the IMSI and GT of serving MSC if the subscriber is available within home network.
- If subscriber is roaming in another network, HLR will send MAP PRN to the VMSC.
- VMSC will acknowledge this message with MSRN, associated IMSI and GT of serving MSC.
- HLR will forward this information to the attacker.

Though GT Numbering of MSC is operator specific, but certain fields are mandatory for routing purpose i.e Mobile Country Code (MCC) and Area Code which could narrow the location of a subscriber down to MSC area. It can be a bigger area in urban localities and a smaller area in populated cities. Other options can be exploited to map MSC codes with a geographical area. Known user locations can be queried by the attacker to map the area with MSC GTs [47]. Moreover MSRN can be used to make a call directly to the subscriber with a local number of the visited country. This will avoid legal interception of call by home network and roaming charges.

3) Short Message Services(SMS): SMS sending/ receiving mechanism is completed in two parts [79][95]. Mobile Originating (MO) Short Message Service transfer and Mobile Terminated (MT) short message service transfer is described as under:

- Subscriber A types a message and sends it to MSC via BTS which includes text of short message, recipient MSISDN and address of SMSC.
- MSC sends MAP MO Forward Short Message to the specified SMSC. SMSC sends acknowledgement of successful storage of this message.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

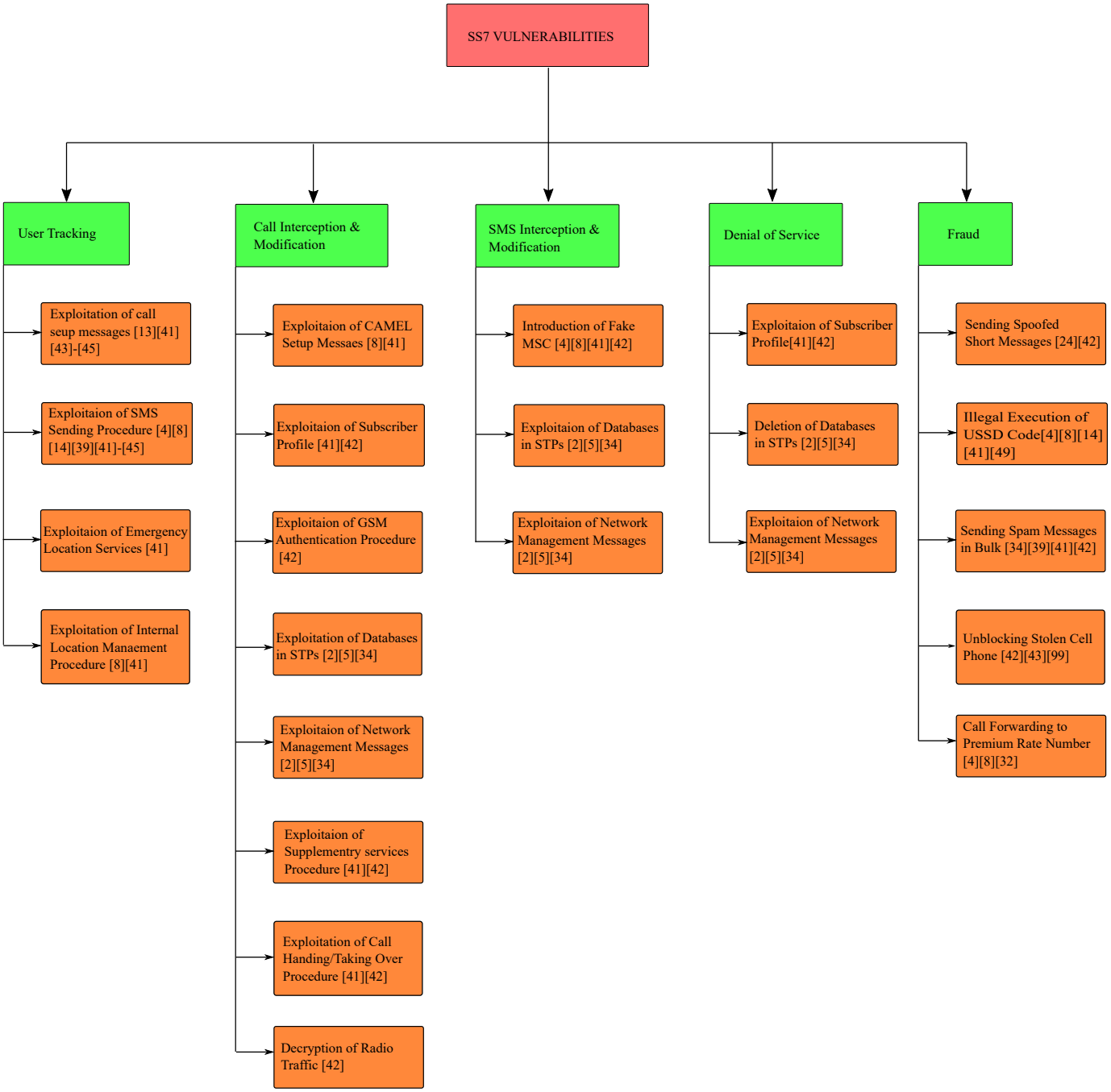


Fig. 8. SS7 attack vectors - This schematic diagram shows list of known methods which can be used to exploit the SS7 network vulnerabilities.

- SMSC has only MSISDN of the recipient. It needs IMSI of recipient and GT of serving MSC to forward this short message to the destination. This information is stored in HLR of recipient.
- SMSC sends MAP Send Routing Information for Short Message (MAP SRI SM) request to HLR of recipient which indicates SMSC wants to send a short message to the indicated subscriber and needs its corresponding IMSI and address of serving MSC.
- HLR replies with MAP SRI SM acknowledgement to SMSC which contains IMSI and GT of serving MSC. SMSC forwards short message to the serving MSC which in turn forwards the message to the recipient.
- If the subscriber is roaming outside the network, then HLR sends MAP PRN request to the MSC in the roaming network which acknowledges with the MSRN. This information along with IMSI and GT of serving MSC is forwarded to the SMSC. SMSC then forwards short message directly to the serving MSC in the roaming network.

4) Exploiting SMS Procedure for Location Tracking: By exploiting SMS procedure, the attacker will be able to retrieve IMSI and GT of serving MSC as shown in Fig. 10. This attack is described as under:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

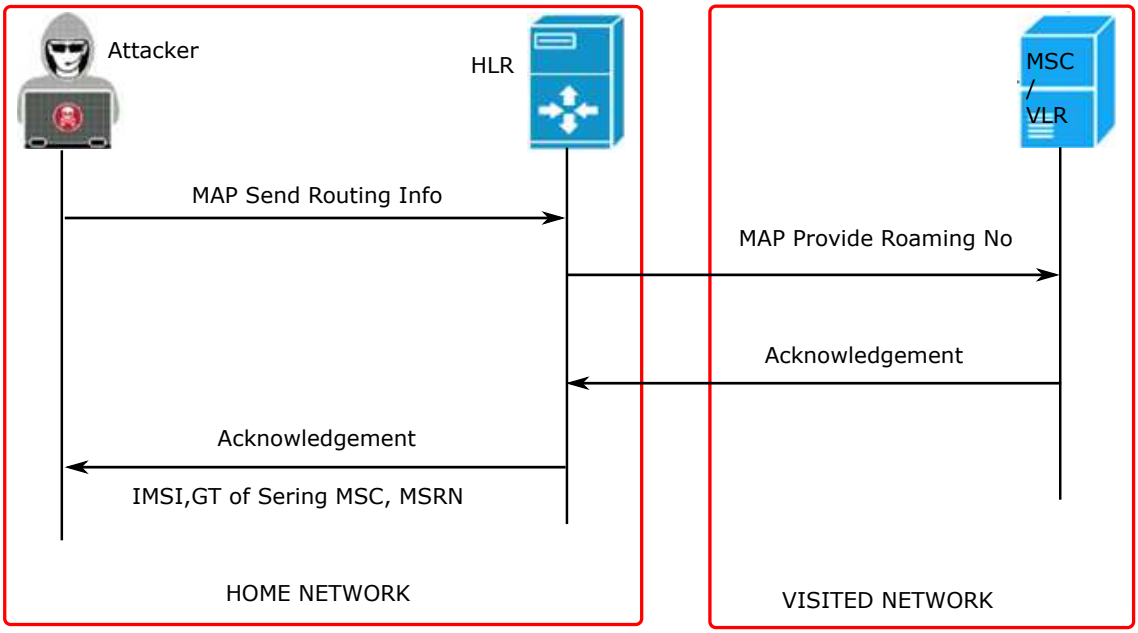


Fig. 9. Location disclosure by exploiting call setup messages [13] - In this method, attacker impersonates as GMSC and asks HLR for whereabouts of victim. HLR replies with IMSI of the user and address of serving MSC where victim is present.

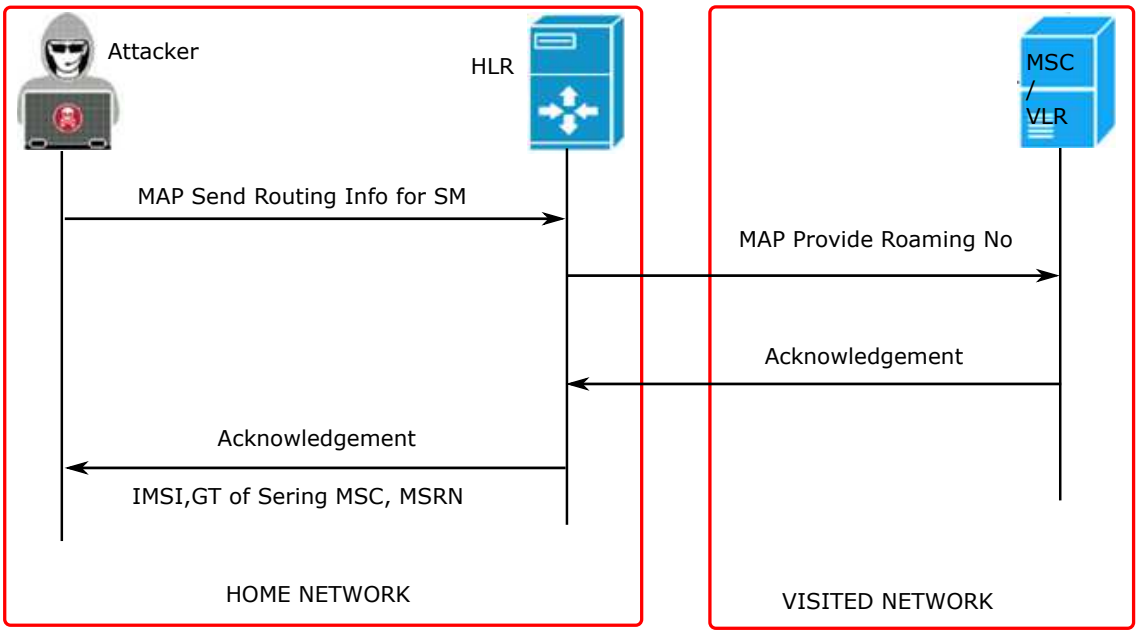


Fig. 10. Location disclosure using SMS procedure [46] - In this case, attacker impersonates as SMSC and asks HLR for address of victim, indicating that it has a short message for victim. HLR replies with IMSI and address of serving MSC.

- Attacker impersonates as SMSC and sends MAP SRI SM message to recipient's HLR which shows that SMSC has a message for recipient.
- As there is no authentication, HLR replies with associated IMSI and GT of serving MSC.
- If subscriber is roaming in another network, HLR obtains MSRN through MAP PRN request and forwards details to the attacker.

5) Internal Location Management Using CAMEL Messages: Service operators can use CAMEL [96] messages to know the location of a subscriber for internal management and to provide location to certain applications which require the position of the subscriber. MAP Any Time Interrogation (MAP ATI) message is used for this purpose. The normal message flow [97] which takes place for the above mentioned service is as under:

- GSM Service Control Function (gsmSCF) sends MAP ATI message to HLR which contains MSISDN of a subscriber.
- As every message is considered legal in the SS7, HLR

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

has address of serving MSC but not the exact location. HLR sends MAP Provide Subscriber Information (MAP PSI) message to the serving MSC/VLR.
- MSC sends a paging request to check the latest location of cell phone. If cell phone is on a call then current location is forwarded otherwise location at which MSC served it last time is forwarded.
- MSC acknowledges MAP PSI message which contains associated IMSI and cell ID where the subscriber is located to HLR.
- HLR sends MAP ATI acknowledgement message to gsmSCF which contains the above mentioned information.

6) Exploiting Internal Location Management Procedure for Tracking: Internal location management procedure can be exploited by following method as shown in Fig. 11

- The attacker with the SS7 access sends MAP ATI message impersonating as gsmSCF to HLR to get cell ID and IMSI of the subscriber [46].
- HLR considers it as a legitimate request and sends MAP PSI to serving MSC/ VLR which determines the location of subscriber through paging request and returns position to HLR. At the end; HLR forwards IMSI, serving MSC GT, and cell ID to the attacker which can be translated into geographical area. This attack is more precise than previous attacks as it reveals additional information of cell ID of the subscriber along with GT of serving MSC, associated IMSI, and IMEI of the subscriber.

7) Combination of SMS and Internal Location Management Attacks.: Some network operators have started to block MAP ATI message due to security and privacy concerns since 2015 [46]. If this message is blocked, HLR will not respond to MAP ATI message. However the attacker can query location of a subscriber directly from MSC bypassing HLR. It requires IMSI and GT of serving MSC which can be obtained through short message attack (MAP SRI SM). The attack sequence is shown in Fig. 12:

- Attacker impersonates as SMSC by sending MAP SRI SM request to HLR for serving MSC address of subscriber .
- As described earlier, HLR provides associated IMSI and GT of serving MSC/ VLR without any check/ authentication.
- In next step, attacker impersonates as HLR and sends MAP ATI message to the serving MSC/VLR.
- MSC sends a paging request to check the latest location of cell phone considering it as a legitimate request.
- After receiving the latest location, MSC forwards MAP ATI acknowledgement message to the attacker which contains IMSI and cell ID where subscriber was served last time/ being served

8) Requirement of Emergency Location Service (LCS): Emergency services need the exact location of the calling party to provide immediate assistance as per location services guidelines [98]. The exact location can be found by different methods like forwarding the GPS location or through triangulation method. This procedure is initiated from the user side to facilitate the location of the user in distress. Same can be done from network side as well, which is used to track suspicious targets by law enforcement agencies. The scope of this paper is to analyse attacks from network side because the attacker is within the SS7 network and is acting as one of the entities of the core network, so we will discuss this scenario only.

9) Legitimate Procedure of Emergency Location Services from Network Side: Normal procedure for emergency location services is described as under [99]:

- From network side, a legitimate client (law enforcement agency) needs to know the position of a subscriber. It sends a MAP Location Based Services (MAP LBS) request from authorised interface to Gateway Mobile Location centre (GMLC).

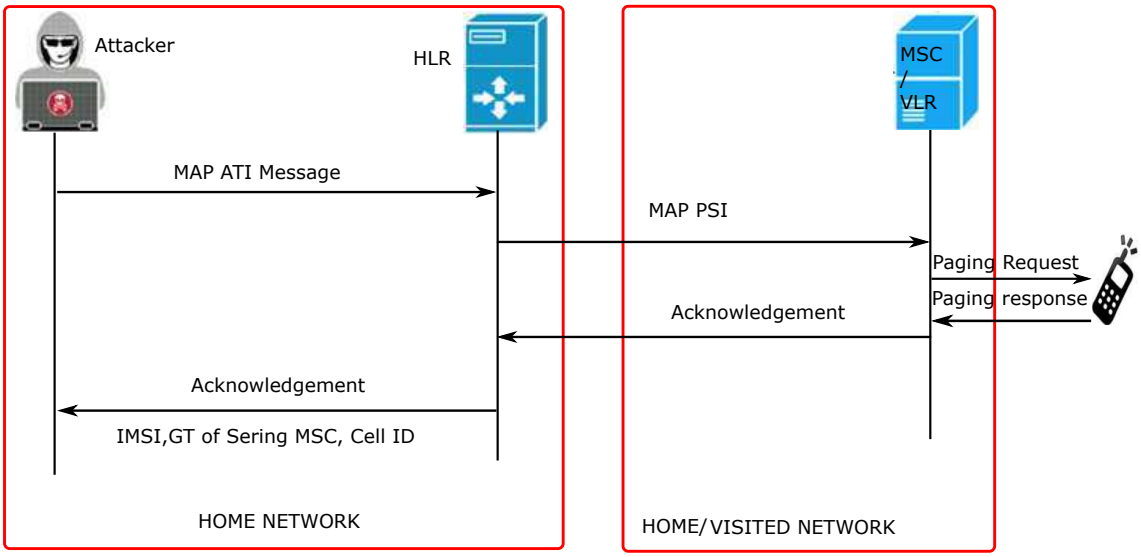


Fig. 11. Location disclosure using ATI message [46] - Attacker gets cell ID and IMSI of the subscriber by sending MAP ATI message, impersonating as gsmSCF. HLR considers it as a legitimate request and sends MAP PSI message to serving MSC/ VLR which determines the location of subscriber through paging request and returns position to attacker through HLR.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

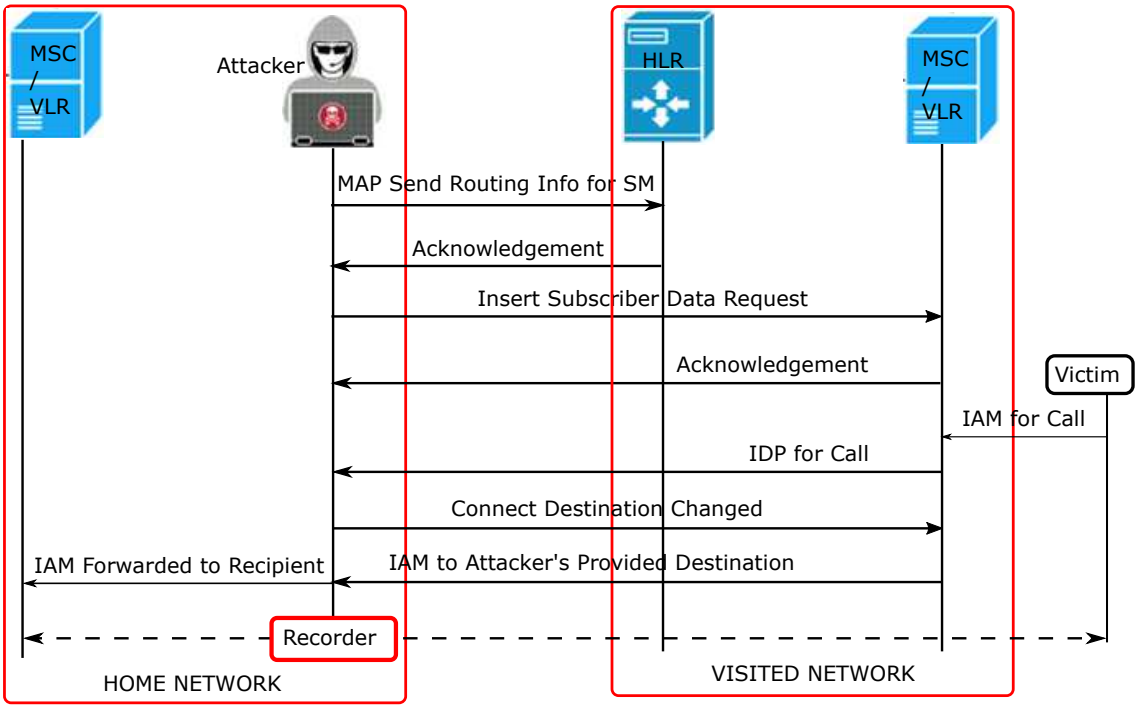


Fig. 12. Location disclosure using hybrid attack [13] - It is combination of SMS and Internal Location Management Attacks. Attacker impersonates as SMSC and gets serving MSC address of subscriber by sending MAP SRI SM request. Then, attacker impersonates as HLR and sends MAP ATI message to the serving MSC/VLR. MSC sends a paging request to check the latest location of cell phone. It returns IMSI and cell ID of the subscriber.

- GMLC authenticates the requesting entity. After successful authentication, it sends MAP SRI LBS request to the HLR.
- HLR replies with MAP SRI LBS acknowledgement to GMLC which contains the GT of serving MSC/ VLR in either own network or visited network in case of roaming subscriber (it will also contain MSRN).
- GMLC sends Provide Subscriber Location request to the

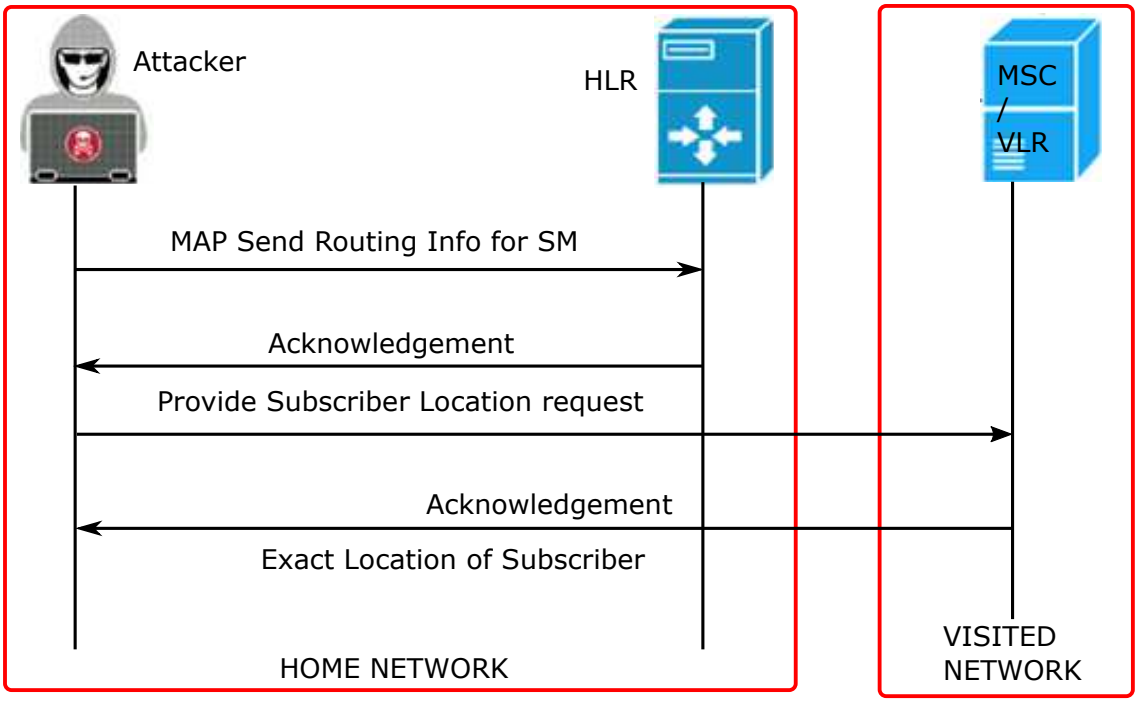


Fig. 13. Location disclosure using LCS message [13] - Attacker gets IMSI and address of serving MSC from HLR. Then, attacker impersonates as GMLC and sends Provide Subscriber Location request to the serving MSC. Serving MSC returns location of victim to the attacker.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

serving MSC.
- MSC sends Perform Location Request message to BSC. BSC forwards this request to Serving Mobile Location Centre (SMLC) which performs location request using Radio Resource LCS Protocol [100].
- Upon receiving exact location, SMLC answers with Perform Location Request Response to MSC which forwards this information to GMLC.
- GMLC forwards location of subscriber to the client.

10) Exploiting Emergency Location Services for Tracking: As we have seen in the normal LBS services procedure, verification of requesting entity is done by GMLC. The attacker needs to bypass this verification [10]. Attacker completes this task by adopting following method as shown in Fig. 13:

- The attacker sends MAP SRI SM containing MSISDN, impersonating as SMSC, to get associated IMSI and address of serving MSC from HLR.
- After receiving this information, the attacker impersonates as GMLC and sends Provide Subscriber Location request to the serving MSC.
- Serving MSC considers it a legitimate request and proceeds as per normal procedure described above and obtains exact location of victim. At the end MSC forwards exact location of subscriber to the attacker.

Attacks discussed up till now show that an attacker can retrieve IMEI, IMSI, GT of serving MSC, and cell ID of a subscriber. The attacker can adopt various methods to pin point the location or to translate this information into a geographical area as under:

- Mapping of MSCs with areas can be obtained from internal compromised sources of the network.
- Some useful information may be available at public databases which can be queried to get desired information i.e using SHODAN search engine [101].
- Third party APIs [102] can be used to translate this information into longitude and latitude of the area.

B. CALL INTERCEPTION SCENARIOS

In this section, possibilities to intercept calls, by using the SS7 vulnerabilities, by the attacker are discussed.

1) Normal Call Setup Procedure For Roaming Subscriber: Requirement of connectivity with a single SIM throughout the world leads to the roaming agreements between different network providers from different parts of the world. This facility is provided through CAMEL services [96]. In this facility, one network operator provides its services to visiting subscribers from other networks and manages these services through CAMAL Application Part (CAP). Basic call setup during roaming is as under:

- When a user enters in a roaming network, she registers herself with one of the MSCs (Visited MSC) of roaming network with which the home network has roaming agreement.
- VMSC sends MAP Update Location Request to HLR of subscriber's home network. This message contains GT of VMSC along with other parameters.
- HLR saves the address so that all calls and short messages can be routed through that VMSC for the subscriber in future.
- HLR sends MAP Insert Subscriber Data message to VMSC which contains subscriber's profile information, security details and address of its gsmCSF with a list of events to be reported to the home network for the particular subscriber.
- If the subscriber makes a call to home country without country code, VMSC does not recognise the format of dialled number and asks gsmCSF of subscriber's home network about instructions regarding the call. gsmSCF converts the dialled number from local format to international format by inserting country code and tells VMSC to forward the call on the modified number.
- VMSC forwards this call to the MSC of called party.

2) Exploiting Roaming Procedure for Interception of Calls: Roaming procedure is exploited by following method as shown in Fig. 14[46]:

- First of all, the attacker needs to know the address of serving MSC, IMSI, and MSRN of the subscriber.
- The attacker impersonates as SMSC and sends MAP SRI SM request to HLR. HLR returns IMSI, MSRN and GT of serving MSC.
- In next step, the attacker acts as home HLR and sends MAP Insert Subscriber Data to VMSC which contains a list of events and address of malicious gsmSCF at which those events need to be reported.
- When the subscriber makes a call without country code, it sends an ISUP Initial Address message (IAM) message to the VMSC.
- VMSC forwards this request to the attacker's controlled gsmSCF/ entity considering it as a legitimate address. The attacker changes the dialled number with that of her own choice and returns the modified number to the VMSC asking it to forward call to this number.
- VMSC forwards call to the attacker's provided number which can be a recording proxy. The attacker has the actual destination number, she can forward the call to the recipient and can record/ listen to the conversation through that proxy. The call is connected but none of the parties involved in the call know about interception.

3) Interception of Incoming Calls - Exploiting Supplementary Services (SS): The SS7 messages are also used for supplementary services like call forwarding and call number display. MAP Register SS message is used to allow call forwarding to a particular number [46]. The attacker having access to the SS7 network can use this message to enable call forwarding for a particular subscriber to a destination of her choice which could be a recording proxy. The message flow of the attack is shown in Fig. 15:

- Attacker needs the IMSI and address of serving MSC of the victim. She gets this information by carrying out short message attack (MAP SRI SM).
- Attacker acts as HLR and sends MAP Register SS message to MSC indicating to enable call forwarding to a particular number. As there is no inherent security control,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

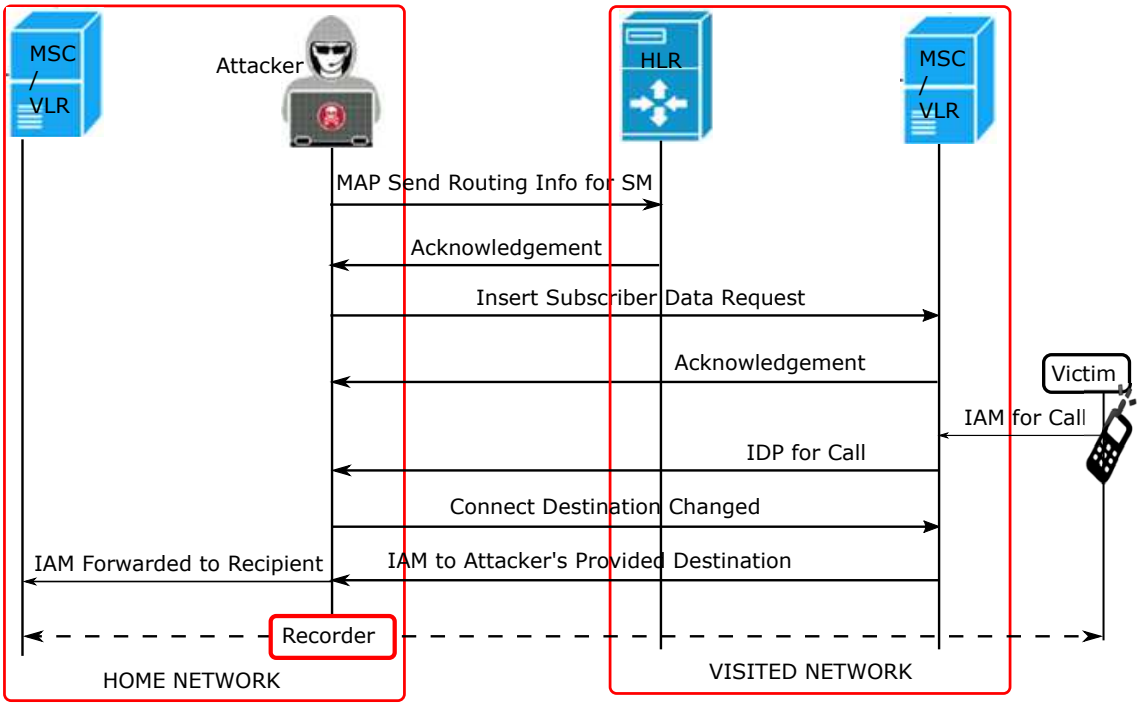


Fig. 14. Call interception by exploiting roaming procedure [47] - Attacker gets address of serving MSC, IMSI and MSRN of subscriber. Then the attacker acts as home HLR and sends MAP Insert Subscriber Data to VMSC which contains a list of events and address of malicious gsmSCF at which those events need to be reported. All those events related to the victim will be reported on address given by attacker.

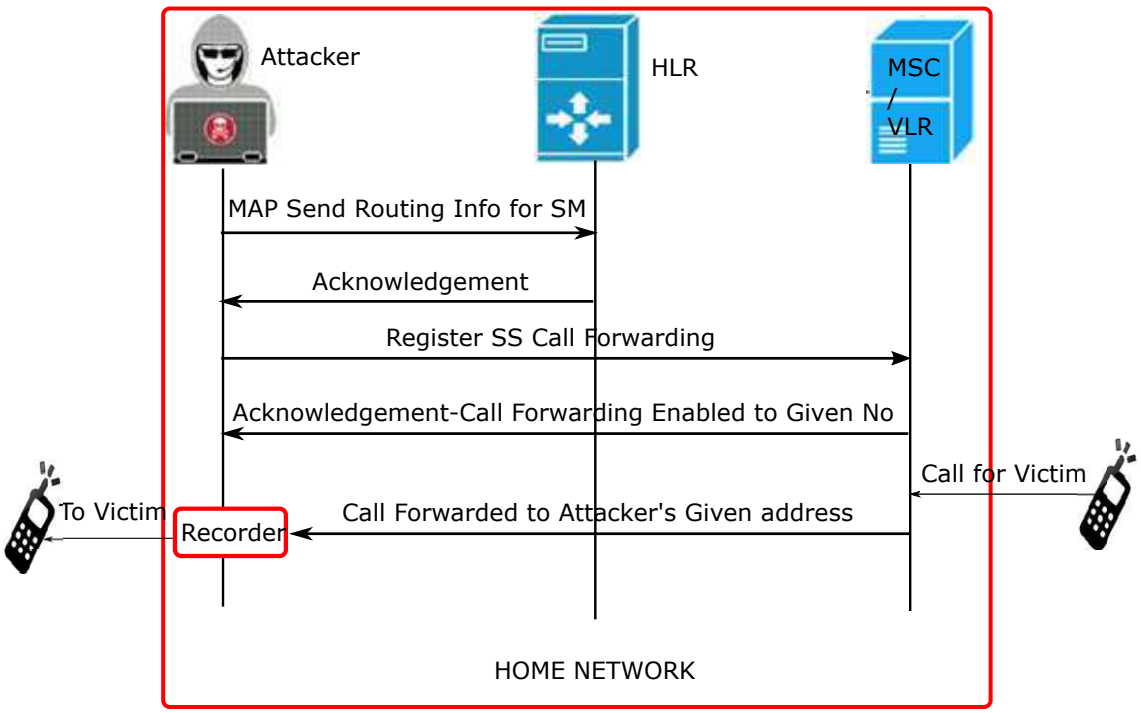


Fig. 15. Exploiting supplementary services[46] - Attacker gets IMSI and address of serving MSC of victim through MAP SRI SM. Then attacker acts as HLR and sends MAP Register SS message to MSC indicating to enable call forwarding to a particular number.MSC enables call forwarding to the desired number. All calls of victim will be forwarded to attacker's given number.

MSC enables call forwarding to the desired number and acknowledges the message.

- Once a call is received for the victim, MSC forwards call to attackers provided number in previous step.
- Attacker can record and forward the call to the victim. MAP Erase SS message can also be used by the attacker to disable call forwarding.
- Attacker enables the call forwarding to her own premium

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

rate number and then calls the victim. Call will be forwarded to premium rate number for which the victim will be charged.

4) Interception of Outgoing Calls - Exploiting Subscriber Profile Using Roaming Procedure: In this attack, the attacker exploits subscriber's profile for interception of outgoing calls. Incoming calls cannot be intercepted by the attacker through this method. Message flow of this attack is as under:

- Attacker needs to know the IMSI and GT of the serving MSC of the subscriber for which she intends to intercept calls. She gets this information with MAP SRI SM request from HLR.
- Attacker acts as MSC and sends MAP Update Location Information message for the victim subscriber to HLR, which shows that the subscriber is being served by that MSC.
- HLR considers that subscriber has moved to the new area and is now being served by the MSC which has sent the message. It sends MAP Insert Subscriber Data message to the attacker which contains security related, and subscriber profile information (subscription package, address of billing platform, and other details).
- Attacker notes down the contents of this message and sends another MAP Update Location Information message to HLR which contains the address of actual serving MSC which was retrieved in first step.
- HLR sends MAP Insert Subscriber Data message to MSC. It is considered a legitimate message as MSC assumes the user has changed her package subscription.
- The attacker impersonates as HLR and sends another MAP Insert Subscriber Data message to MSC with the same contents as noted in step 4, except for the address of billing platform which is replaced with a malicious address. MSC again accepts the changes by taking it as a change in subscription package by the user.
- When victim makes a call, MSC forwards Initial Detection Point (IDP) message to billing platform for charging purposes. The address of billing platform is malicious and is controlled by the attacker. Attacker rewrites the number with one of her proxies and allows MSC to forward call to the new number.
- MSC sends IAM to the destination which is a recording proxy set up by the attacker. This proxy connects the calling party with destination and records all calls in the middle. As the call is finally being forwarded to its destination, so the victim never knows that her call is being recorded or intercepted.

5) Intercepting Calls by Decrypting Radio Traffic.: Radio traffic of a user can be decrypted by the attacker in following way:

- When a subscriber enters in new MSC area while making a call (on the move), a series of messages are exchanged between two MSCs to provide seamless handover of call from one MSC to othe MSC.
- In such a scenario, already established identities and session keys are used to continue the call. New MSC sends MAP Send Identification Message request for the subscriber to the old MSC.
- Old MSC sends encryption keys which are being used in this call so that the subscriber does not need to establish new keys for same call [44]. New MSC receives these keys and when call is handed over, it uses these keys to manage the call.

The attack proceeds as follows and is depicted in Fig. 16:

- The attacker intercepts call on air interface using some custom made device for this purpose. The Attacker needs to be in the vicinity of the victim. As call is encrypted, the attacker needs the decryption keys to decrypt it.

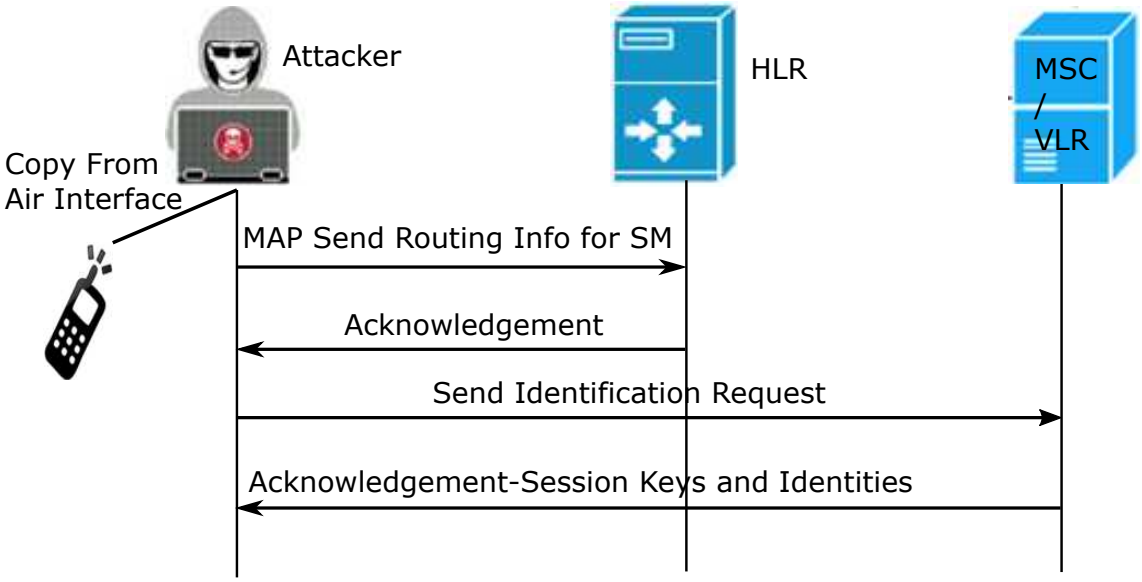


Fig. 16. Intercepting calls by decrypting radio traffic [47] - Attacker intercepts encrypted call on air interface. Attacker impersonates as MSC and gets session keys needed to maintain the call by sending MAP Send Identification message to serving MSC for taking over the call. serving MSC shares session keys with the attacker.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

- Using MSISDN of the victim, attacker retrieves IMSI and GT of serving MSC from HLR through MAP SRI SM attack impersonating as SMSC.
- The attacker impersonates as MSC and sends MAP Send Identification message to serving MSC. Serving MSC considers that the subscriber is moving and entering into a new MSC area.
- Serving MSC initiates the call handing over procedure and acknowledges with the session keys needed to maintain the call.
- The attacker receives the keys and is already copying call on air interface, the handover never takes place and attacker can decrypt the call in a live attack or can save the call to decrypt it later [44]. Temporary Mobile Subscriber Identity (TMSI)can provide some defense in identifying the particular user over air interface. It is assumed that the attacker has gained TMSI through some other method which is out of scope of this paper.

C. SMS INTERCEPTION AND FRAUD CASES

There are numerous SMS fraud cases, however, in this section only those cases are discussed which exploit loopholes in the SS7 network.

1) SMS Interception Using Fake MSC: A Short Message Service (SMS) is delivered in two parts in following way:

- Sender sends the short message to the SMSC through MSC which is called Mobile Originated (MO) part.
- SMSC forwards this short message to serving MSC which subsequently delivers it to the recipient and is called Mobile Terminated (MT) part.
- It is prudent to mention here that mobile originated forward short message received by SMSC has no authentication mechanism and therefore can be exploited by the attacker for malicious purposes.
- In this attack, the aim of the attacker is to receive, store, modify all short messages of a particular subscriber, and then forward these messages to the recipient. Message flow of attack is shown in Fig. 17. The attacker impersonates as SMSC and sends MAP SRI SM for a subscriber to HLR by enclosing MSISDN of the subscriber.
- HLR acknowledges with MAP SRI SM reply which contains the IMSI and GT of the serving MSC.
- The attacker has learned IMSI and GT of serving MSC. Now the attacker acts as VMSC and sends MAP Update Location message for that subscriber using received IMSI to home HLR. This message shows that subscriber is being served by that VMSC. HLR saves the address of the VMSC for future.
- When another subscriber sends a short message to the victim, SMSC of sender contacts HLR of the victim through MAP SRI SM request.
- HLR has the address of victim which was provided by the attacker as serving MSC. It forwards the same to SMSC in acknowledgement message as the GT of serving MSC for the victim.
- Sender's SMSC forwards short message to the fake MSC which is received by the attacker who can copy, modify, and then forward it to the actual recipient.
- The victim number is continued to be compromised until she enters into a new MSC area and her location is updated to the HLR. Until then the attacker intercepts all short messages of the victim including one time passwords for financial transactions, authentication codes from social networks, and other important messages.

2) Exploiting Mobile Originated Forward SM Part: As there is no authentication check on mobile originated forward short messages and mobile terminated forward short message parts, they can be exploited by an attacker having access to the SS7 network. This attack can be used for a variety of purposes like sending spam messages for commercial purposes and fake messages or flooding (short messages) attack on a particular subscriber. This attack can be described as under as shown in

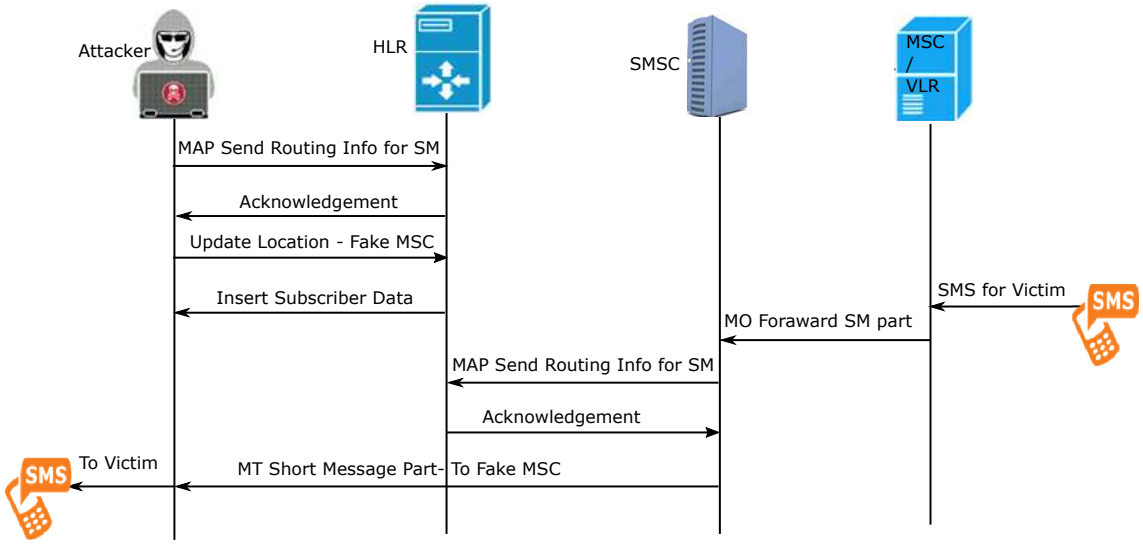


Fig. 17. SMS interception using fake MSC [47] - Attacker impersonates as SMSC, gets IMSI and address of serving MSC of victim. Then attacker acts as VMSC and replaces address of victim with fake MSC in HLR. All short messages will be forwarded to the fake MSC controlled by attacker.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

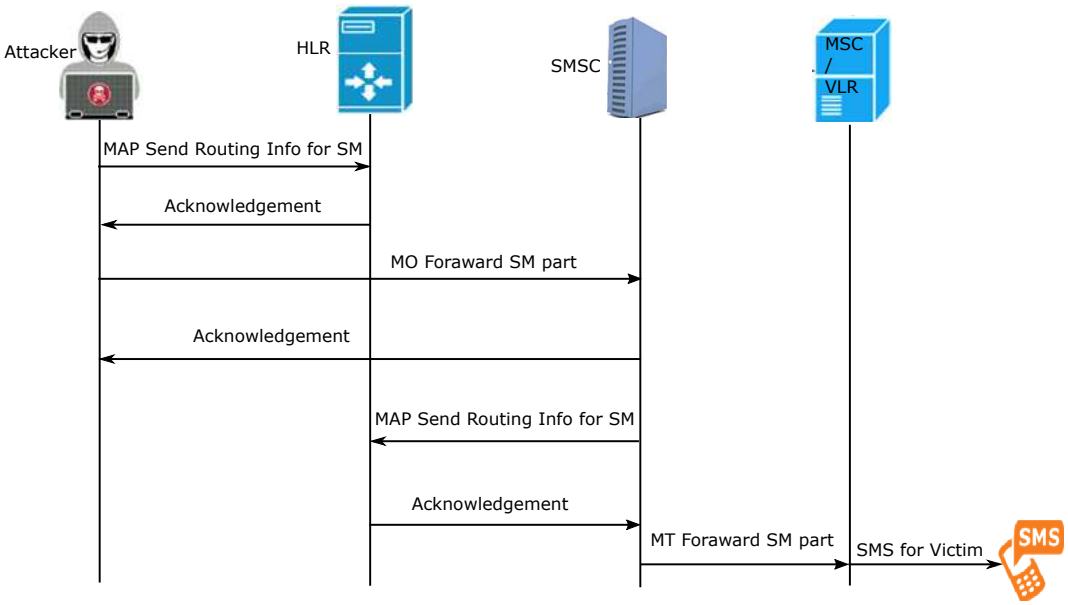


Fig. 18. Exploiting MO forward short message part [47] -Attacker gets IMSI and address of serving MSC for victim through MAP SRI SM. Then, attacker acts as serving MSC for the user on whom behalf she is sending the short message, and forward mobile originated short message part to SMSC. This message is sent to recipient.

Fig. 18:

- If attacker wants to send a short message to a subscriber on behalf of another subscriber, she needs to know the IMSI and address of serving MSC for both the subscribers. This information is obtained by sending MAP SRI SM to HLR.
- The attacker acts as serving MSC for the user on whom behalf she is sending the short message and sends mobile originated forward short message part to SMSC.
- SMSC forwards this message to the recipient. SMSC sends message MAP SRI SM to HLR. HLR replies with MAP SRI SM acknowledgement which contains the address of serving MSC and IMSI of the recipient.
- SMSC forwards mobile terminated forward short message part to the serving MSC which subsequently delivers it to the recipient.
- In this way, messages can also be sent anonymously to send large number of spam messages for commercial purposes and can be used to send a flooding attack on a particular subscriber.

3) Unblocking a Stolen Mobile Phone.: In this attack, the purpose of the attacker is to unblock and use a stolen cell phone for financial gains or other malicious intents. The attack proceeds as follows [103]:

- When a cell phone is switched on, it starts registration process with the network.
- Cell phone sends IMEI number to MSC through BTS. MSC sends MAP check IMEI message to EIR to checks status of IMEI (Black, white or grey). EIR forwards the results with MAP Check IMEI acknowledgement message to MSC.
- Based on this result, MSC decides to allow or deny access to cell phone.
- During attack, the attacker turns on a check in EIR, which mandates EIR to check the associated IMSI which was being used when IMEI was blocked, if the IMEI is in black list.
- It is assumed that the attacker has the IMSI of the stolen phone which was associated to it when it was blocked.
- Attacker impersonates as MSC and sends MAP Check IMEI message to the EIR with IMEI of the stolen phone and IMSI which was associated with it before it was blocked.
- EIR checks IMEI which will be in blacklist and then checks associated IMSI and compare both IMEI-IMSI pairs when mobile was blocked and the pair received in previous step.
- Both the pairs are same, so the EIR moves the IMEI to the white list considering it was blocked due to some error or the owner had found the lost cell phone. Now the attacker can use any SIM with that cell phone as its IMEI is moved to the white list.

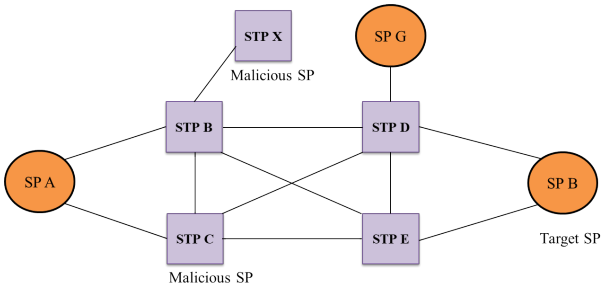


Fig. 19. Exploitation of network management messages [2] - Attacker sends a malicious Changeover Order message to STP B impersonating as SP A. STP B assumes the message is legitimate and stops sending signalling messages to the link reported unavailable in Changeover Order message by the attacker.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

4) Transferring Funds Using USSD: Some service providers are giving option of sharing credit through Unstructured Supplementary Service Data (USSD). USSD code is executed by the subscriber to send or share the credit [46]. An attacker having access to the SS7 impersonates as a subscriber and sends MAP Process USSD message which is executed without any authentication.

D. DENIAL OF SERVICE (DOS) ATTACKS

DoS attack aims to disrupt the services for a particular subscriber. When a subscriber moves to a new area and gets registered with a new MSC, it sends MAP Update Location message to HLR. After receiving this message, HLR sends MAP Insert Subscriber Data message to MSC/ VLR [76]. This message and MAP Delete Subscriber Data message is also sent to MSC/ VLR when a subscriber changes her subscription package. These messages contain the details of all activities, a subscriber is allowed/ not allowed to do. Attacker can use these messages to deny the subscriber from making/ receiving calls and sending/ receiving messages [46] in following way:

- Attacker collects IMSI and GT of serving MSC through short message attack (MAP SRI SM).
- Attacker acts as HLR and sends MAP Insert Subscriber Data/ Delete Subscriber Data message to MSC.
- This message contain the instructions that subscriber is not allowed to make/ receive calls and send/ receive short messages.

E. EXPLOITING NETWORK MANAGEMENT MESSAGES

At MTP 3 layer, network management messages are exchanged between two directly connected STPs via C-link to determine/ convey the status of a route or an SP with respect to congestion/ non-availability. These messages have no inherent authentication and integrity check and can be exploited by the attacker. There are various network management messages used at this layer but two of them are be discussed in this section.

1) Changeover Procedure: When a signalling link fails or becomes unavailable for signalling traffic, Changeover procedure is used to re-direct signalling messages from alternate routes which are available to that destination. The failure is detected due to high signal error rate, prolonged delay in acknowledgement of sent messages, congestion, and unavailability of terminal equipment [104]. When this scenario is detected by an SP and needs to carry out a Changeover Procedure, it sends a Changeover Order message to the connected SPs. No inherent authentication, encryption or integrity mechanism is involved. The receiving SP checks only the routing label of the sender (originator address). If routing label is one of the directly connected SPs, the message is considered legitimate otherwise it is discarded.

Exploitation of Changeover Procedure: We consider the scenario presented in Fig. 19. Let us suppose STP X is under control of the attacker and can send malicious management messages to other nodes [2]. It sends a Changeover Order message to STP B impersonating as SP A (uses routing label of SP A). STP B has the only way of checking the legitimacy of the message is by checking routing label. STP B assumes the message is legitimate and stops sending signalling messages to the link reported unavailable in Changeover Order message by the attacker. If the attacker has capability of sending multiple messages to STP B with coordination from other nodes, she can make some signalling links unavailable. Traffic will be diverted to alternate routes consuming more resources and decreasing efficiency.

2) Transfer Prohibited Procedure: When a particular destination is unreachable to an STP, it initiates Transfer Prohibited Procedure (TFP). In this procedure, it informs to adjacent SPs about the unavailability of a particular destination and to stop forwarding messages for that destination. A TFP message contains following information [104]:

- Routing label of the originating STP.
- Transfer prohibited signal.
- Destination address for which messages are not to be forwarded due to its unavailability.

We consider the scenario given in Fig. 19. STP D has two routes to transfer messages to SP B. It can deliver messages directly to B or via STP E. If both the routes become unavailable, STP D can no longer send messages to SP B. STP D initiates TFP message to adjacent SPs notifying them SP B is not available and its messages are not to be routed through it. All the messages at STP D destined for SP B are dropped. If there is no alternate route available to other STPs, they also drop messages destined to SP B.

This procedure can be exploited by an attacker. We consider SP B is target SP of the attacker. Initially all links are working and two routes are available for messages destined to SP B. let us say attacker controls the STP X and sends a malicious TFP message to STP B impersonating as STP D. It contains the address of SP B as unavailable destination. Now all the messages of SP B will be routed through STP E. It has provided the chance to attacker for traffic diversion. If the attacker has ability to generate multiple messages or coordinated messages, she can send TFP messages impersonating as STP E which also declares SP B unavailable. Then all the messages from STP B which are destined to SP B will be dropped; creating a denial of service for SP B.

F. COMPUTER ATTACKS ON CORE NETWORK ELEMENTS[28].

The attacker can gain full control of the databases/ core network elements by attacking Operation Support System (OSS) or remote access application. This situation could be devastating in many ways as follows:

- Re-routing of calls by exploiting and changing various data bases and customer's record in the SS7 network such as changing call forwarding and speed dialling numbers of a particular subscriber or random changes in the data base to create a chaos.
- Exploiting routing tables and GT translation tables gives opportunity to record calls by forwarding them to the desired location/routes.
- Interception of secret user identities by deploying the SS7 packet sniffers due to no encryption in the core network.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

- Deletion of routing tables, GT translation tables, call forwarding data and speed dialling information stored at various databases can cause interruptions.

These attacks can cause havoc at national level especially in those countries where only few telecom operators provide services in the country and each company provides services to a large portion of population as compromise of one company will effect a major part of population. Just take the case of altering call forwarding data base. An attacker alters the call forwarding data base and sets all call forwarding to emergency services at the time of a major crises like a terrorist attack or a natural disaster. It can create a panic because all normal calls will be forwarded to emergency service centre. This will create a chaos in the public and can cause delay in rescue efforts. If GT data base is altered, then the calls will be forwarded to wrong MSCs/ VLRs where the recipient is actually not available hence creating a DoS attack.

V. DEFENSES

Defenses against exploitation of the SS7 network have been proposed by various researchers/ security experts. These defenses have been summarised in table IV. In this section defenses of the SS7 are discussed briefly.

A. Critical Security Controls

Following Critical security controls can help in protecting the SS7 core network [8]:

1) A clear boundary of the network is to be defined. All messages entering and leaving the network needs to be filtered and checked whether they have some external usage or not. The SS7 firewalls and IDS/IPS can be used for this purpose.

2) All the events/ activities and communication in the core network are to be logged for analysis and audit of network. Logs are to be maintained through inherent capabilities of the core network entities or through logging devices deployed within the core network. Logs are to be analysed and audited regularly and results are to be evaluated.

3) Network is to be properly segregated. Trust and exposure level of each element is to be defined and then to be placed in the network accordingly. Different security zones are to be established and the network elements need to communicate with other networks are to be kept in separate security zone.

4) Penetration testing is to be carried out at regular intervals and after addition/ deletion of devices. This helps in finding the vulnerabilities and security gaps of the system. Red team exercises are to be conducted regularly to check system defenses and to improve response time of the team to counter any attack.

5) Attacks on the SS7 network are very likely to occur. It is necessary to maintain and train a team of security experts to respond the incidents in case of an attack materializes.

6) Best practices should be adopted while configuring core network elements. They should be hardened, unused services and accounts are to be blocked, no extra port is to remain open, and all the settings and management related activities are to be done from local control on the core network or through a secure channel.

B. Scrutiny of Signalling Messages

1) MAP insert Subscriber Data message is sent by the home network of the subscriber to the visited network. This message is to be authenticated before saving it for future use. Source network of the message must be checked. Any message which has been originated other than the subscriber's home network is to be drppoed [47].

2) All requests arriving at HLR are to be processed and validated prior giving any information which contains subscriber data such as IMSI and whereabouts.

3) Application layer firewalls are to be deployed to filter out and check MAP and CAP messages leaving or entering the network. Effective policies and monitoring is to be done to get desired results.

4) On the subscriber side, there is very less avenue which can be explored for defense against these attacks. However, there are some applications like "SnoopSnitch" [105] and "Darshak" [106] available to be installed on cell phones which can help in analysis of the subscriber's SS7 traffic and can give warning of unusual activities.

5) MAP ATI messages are used internally for location management and need to be blocked due to privacy concerns. Though some of the service operators in Europe have blocked these messages but most of the operators in the world are still using these messages which can be exploited [46].

6) MAP SRI SM message come from other network and have a legitimate purpose. These messages could be secured from being exploited with the introduction of SMS home routing [107]. Without SMS home routing, these messages are difficult to be identified for their malicious intent.

C. SMS Home Routing

It has been established from attacks explained above that the attacker necessarily needs the IMSI and GT of serving MSC to procced further with her attacks. Both of these identifiers can be obtained by different methods from HLR. One of the easiest methods used by the attacker is with the help of MAP SRI SM. In this scenario the short message is not forwarded to home HLR of the recipient rather SMSC of the sender network asks only about the IMSI and GT of serving MSC of the recipient which is handed over without any authentication. This method is exploited by the attacker and raises serious security and privacy concerns. Realizing these threats 3GPP presented a proposed solution for this problem with the name of home routing published in 2007 [107][114]. SMS sending procedure without home routing is shown in Fig. 20 and SMS sending procedure with home routing is shown Fig. 21. This modification defined a new way of sending short messages. Instead of handing over IMSI and serving MSC GT to the sender, it enabled home network to receive and then forward the short message to the recipient. This modification requires a new entity to be installed by each network provider called SMS-Router. After installation of this router, when an SMSC will send MAP SRI SM to HLR, HLR will not reply rather it will forward this message to SMS router. SMS router will reply with MAP SRI SM Acknowledgement which will be forwarded to sender's SMSC.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

TABLE IV
SUMMARY OF DEFENSES

Reference	Year	Defensive Measure Recommended
F. Oneglia and T. Baritaud [108]	1998	It presents the SS7 network vulnerabilities with respect to access control. As part of the solution, it presents test cases to verify signalling traffic coming into network to ensure filtering and identification of malicious traffic.
IETF Network Working Groups[109]-[111]	1999 2002 2003	SIGTRAN Protocol remained a point of concern for security experts since its introduction. On IP side of the network, IETF's SIGTRAN working groups have suggested use of IP Security (IPSec) and Transport Layer Security (TLS) for protection of interworking vulnerabilities.
G.Lorenz et al[5]	2001	It suggests a generic SS7 attack management system to be used. This network management system comprises of the SS7 firewalls, authentication modules, real time fraud analysers, SCP access control module and packet sniffers.
H. Sengar et al[2]	2005	It presents a secure protocol MTPSec to be used at MTP3 layer to avoid exploitation of the network management messages.
H. Sengar et al[30]	2006	It suggests solution for vulnerabilities arising due to VOIP and PSTN integration. It suggests use of trust management system, authentication module, enhanced firewall solution, IDS and Armour protection for feedback of new vulnerabilities.
H. Sengar et al[32]	2006	It suggests use of MTPSec and IPSec. It has also proposed a generic solution to be used at signalling gateway. This solution consists of enhanced firewall capability providing both syntax and content screening and IDS for anomaly detection.
Chung, Kang [112]	2007	Concept of TCAPSec has been introduced for protection of the SS7 messages. A new entity with the name of Security Gateway (SS7SEG) has been proposed to be used between two interconnection operators for implementation of TCAPSec. While interacting with other operators, all inbound and outbound traffic of an operator is to pass from this SEG. SEG inserts and remove protection in the messages as defined policies. It offers following three modes of protection: • Protection mode 0: no protection. • Protection mode 1: Provision of integrity and authentication. item Protection mode 2: Provision of integrity, authentication, confidentiality.
Lingling, Jiang and Ma Hong [39]	2009	It suggess MTPSec to be used at MTP3 layer. It also suggests use of TCAPSec to provide content authentication, source verification, confidentiality and protection against replay attacks.
An Xinyuan et al [40]	2011	It Suggests improved MTP3 discrimination to protect network management messages. It has also recommended examining of signalling information field to identify illegal network management messages.
Positive technologies [14]	2014	It suggests filtering of messages, monitoring SS7 traffic, finding and fixing configuration errors in the equipment. It. has also offered products PT SS7 scanner and PT IDS-SS7 to help overcome these vulnerabilities
S.P Rao [47]	2015	It suggests a generic approach for mitigation of attacks and recommends good practices to be adopted to safeguard SS7 network from a possible attack.
Hassan Mourad [8]	2015	It suggests some of critical security controls for better protection of SS7 network.
S. Holtmanns et al[52]	2016	It recommends use of SMS home router, basic SS7 filter/firewall for screening of signalling messages. It has recommended implementation of network domain/ IP security at Diameter protocol edge to avoid exploitation.
Kristoffer Jensen et al [48][49][50]	2016 2017	It suggests and presents use of machine learning techniques to detect attacks on SS7 networks. It recommends that anomaly detection techniques are to be used to filter out incoming MAP messages based on various parameters of network and user.
S. Puzankov [55]	2017	It recommends regular vulnerability assessment of the network. External SS7 connections are to be monitored and equipment is to be configured correctly.
Rupprecht, David [113]	2018	It has recommended following security measures: • SS7 penetration testing • Stateful SS7 firewall • SMS home routing • Stateful IP fire walls
Liu C X, Ji X S, Wu J X, et al [57]	2018	It has proposed a defense model with the name of DVM (dynamic and virtual mapping) to address the issue of mapping a user's data inside mobile network. It has suggested dynamic and virtual mapping to conceal the mapping relations of the users identity and other parameters.
Abdelrazek, Loay, and Marianne A. Azer. [58]	2018	They have proposed a framework/ tool (SIG PLOIT) for penetration testing of SS7 network. This tool can be used for detection of Location tracking, interception of call/ sms , fraud cases , DOS attacks, and fuzzing
Qasim, Tooba, M. Hanif Durad et al [59]	2018	They have recommended use of machine learning techniques to detect/ mitigate SS7 attacks.
Aung, Tun Myat, et al [60]	2019	It has proposed encrypted SMS services for android using RC4 stream cipher to avoid SMS interception

Two major differences in the contents of acknowledgement messages with SMS router are:

- IMSI of the subscriber is not sent rather a mapped value from SMS router is sent which is only available with the SMS router. This prevents disclosure of IMSI to the malicious entities/ attacker.
- GT of serving MSC is not forwarded rather GT of SMS router is sent to sender's SMSC and asked to forward short message to this address. This makes the home network overall incharge of short message sending procedure rather than giving control to sender's SMSC.

This method prevents most of the SMS based attacks described earlier like spoofed and spam messages. It also provides the capability of lawful interception of the short messages to the home network if the subscriber is roaming in another network. Previously home network was unaware of the contents of short message if the subscriber was roaming.

D. Use Of MTPSec at MTP3 Layer

Network management messages are exploited due to absence of any security mechanism between adjacent SPs in the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

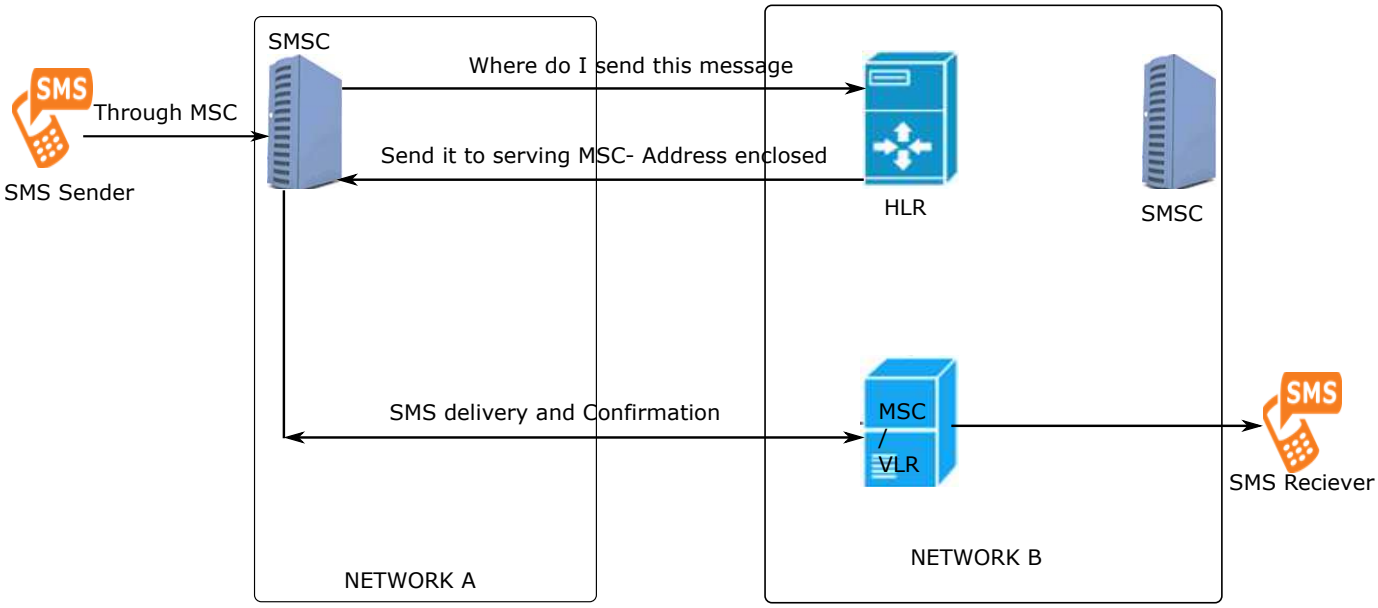


Fig. 20. SMS procedure without home routing [114] - SMSC asks HLR for address of a user to send a message. HLR sends IMSI of the user and address of serving MSC where user is present.

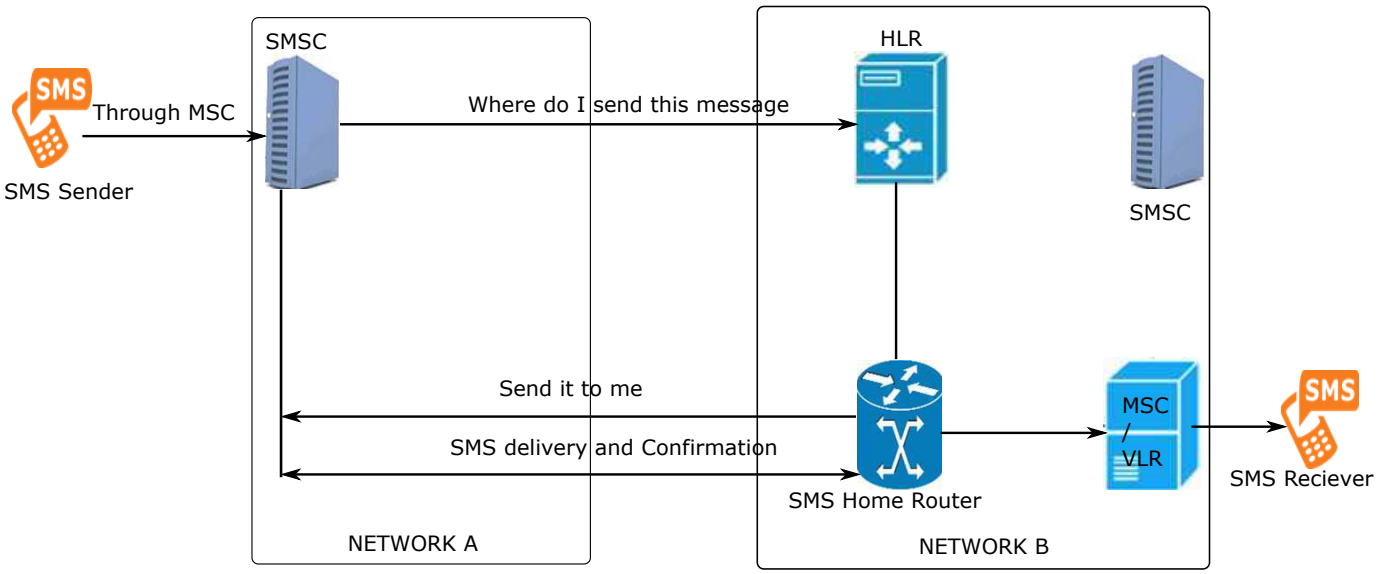


Fig. 21. SMS procedure with home routing scenario [114] - SMSC asks HLR for address of a user to send a message. Address of home router is sent to SMSC. SMSC will send message to home router, home router will forward message to destination. Credentials of the user will not be provided to other network.

SS7 network. To achieve mutual authentication and to enforce integrity, a solution was proposed to be used at MTP3 layer with the name of MTPSec [2]. This solution consists of two protocols namely Key Exchange and Authentication Header protocol. These protocols can be used to provide mutual authentication between SPs, integrity of the contents of the management messages, key generation, and key management.

E. A Conceptual Defense Model

For the prevention and mitigation of attacks, a conceptual model is proposed as shown in Fig. 22, based on the SS7 management system presented in [5] and [47]. This model is in addition to the deployment of SMS home routing by the network provider. The details and specification of the proposed components are left to the network provider to choose from available options in the market or to develop proprietary solutions specific to their needs.

1) Access Control/ Authentication: SSPs are the components of SS7 core network which interact with the subscriber's device. They are the entry points of an attacker as well. There needs to be an access control mechanism to enter into the SS7 network. An authentication module on SSPs will serve the purpose. It should issue an authentication token or key to every legitimate user for access to the network and block all other accesses to the network.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

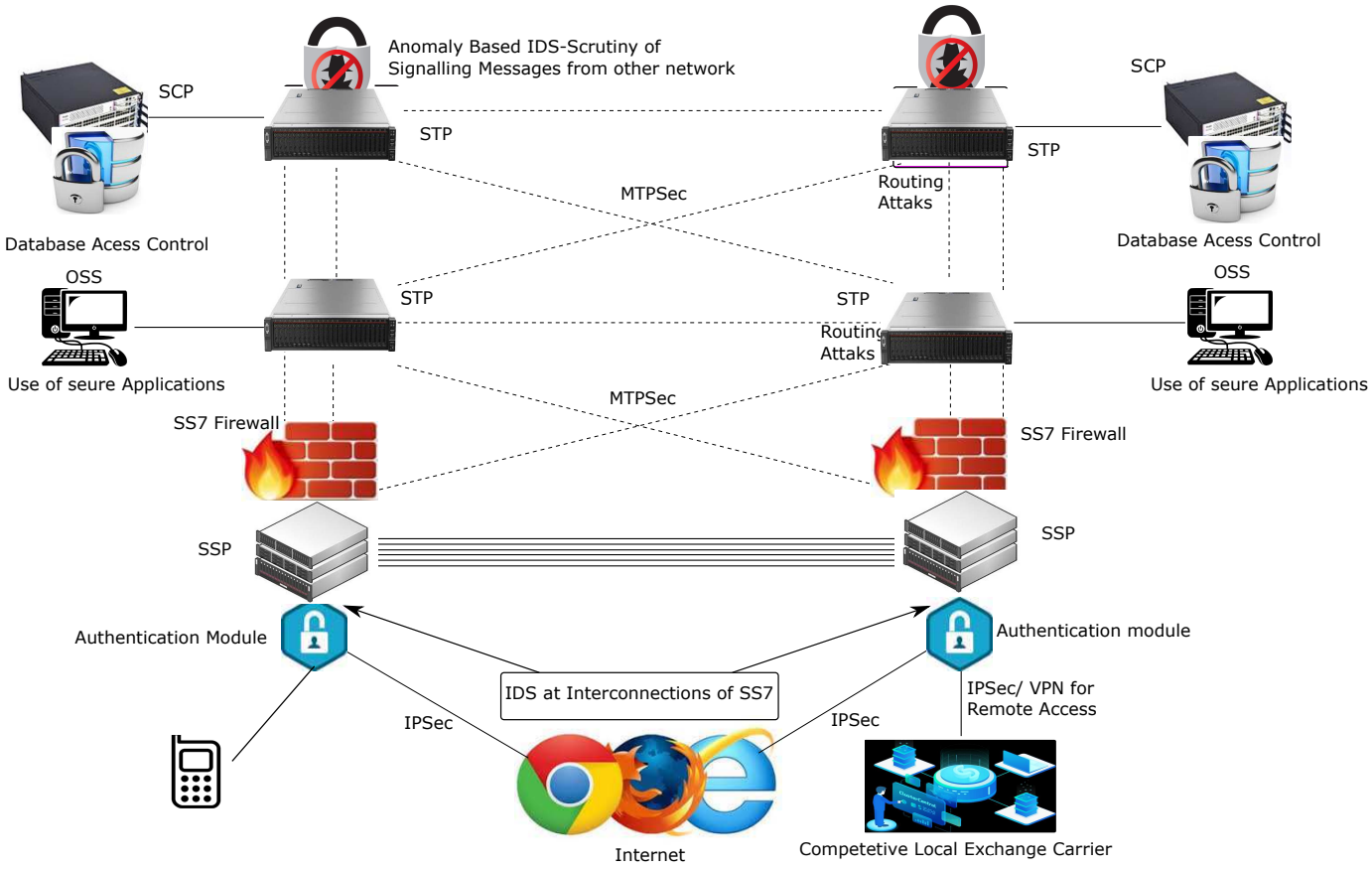


Fig. 22. A conceptual defense model based on [5] - For defense of the SS7 network, access control should be implemented on SCP. Anomaly based detection techniques should be used on STP. MTPSec should be used to avoid sniffing of the SS7 messages. Authentication mechanism should be implemented on SSP. To communicate with IP network, IPSec should be used outside the SS7 network.

2) Encrypted Authentication: For cell phone users, authentication will take place over air interface so it needs to be encrypted with session keys,once the user has been identified by the network. Every time a user requests for a service through SS7 messages, network should authenticate the user with the help of authentication token or key, issued in previous step. This will prevent attacker from exploiting the SS7 network. Messages used for signalling between different components of the SS7 network need to be authenticated. There should be a mechanism to authenticate the contents and origin of the these messages. Cryptographic protocols can be used for this purpose. There is no reason that core network elements cannot support cryptographic applications. The only issue could be the delay in signalling before connecting a call and sending a short message. Elliptic curve cryptography [115] can be used within the core network which is an efficient and lighter encryption system. However for inter-networks communication, concept of PKI [116] can be implemented.

3) Encryption of Signalling Messages: Signalling messages used within the network need to be encrypted so that they are not understood by the attackers if they are intercepted. Attacker needs to map the core network entities for the attack purpose. Encrypted messages will prevent attacker from learning about infrastructure of the core network. Virtual private network (VPN) [117] can be used between interconnecting operators so that interception of these messages can be avoided[47]. Another solution is the use of public key infrastructure (PKI) Certification Authority (CA) [118] for inter-network communication to avoid spoofing and to provide authentication. MTPSec can be used within the SS7 network to achieve security of messages at MTP3 layer.

4) Use of secure protocols for SS7 over IP: As it was discussed earlier, voice and data have been merged and the SS7 protocol has been modified and integrated with other protocols like SIGTRAN. This resulted in sending the SS7 messages over IP. For these messages, secure protocols like IPSec [13] should be used.

5) Deployment of Application Layer Firewall/ IDS/ Scanners: Application layer Firewall can be deployed to filter out the SS7 MAP messages. Moreover, Intrusion Detection system (IDS) [119] and scanners can also be used in addition to the firewalls. These could be used in form of signature detection or anomaly detection. To prevent exploitation of known vulnerabilities, signature detection techniques will be more useful. However, in future as more vulnerabilities will be discovered and new attacks are expected to be disclosed, anomaly detection technique will be more suitable. Firewall can be deployed at STPs [47]. Most of the attacks target STPs impersonating as other network/ roaming partner. Safeguarding the interconnections at STP is one of the most important tasks. While communicating with STPs, the attacker can exploit the inherent weakness of non-availability

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

of security controls within the SS7 network and can ask for important information. However a state of the art Firewall at interconnections can be used to establish a check point on malicious activities. Here machine learning can be employed for anomaly detection.

6) Packet Analyser: A packet analyser can be used in combination with firewall at interconnections of the network. Analysis of results from this analyser can be very useful to tune the firewall for better results and detection of malicious activities[47].

VI. Machine Learning vs Rule Based Filtering for Anomaly Detection

Machine learning based models (supervised and unsupervised learning) vs rule based filtering were implementd on a simulated SS7 dataset to suggest the best possible method for detection of the SS7 attacks/ anomalies. *K* means clustering algorithm, Generalized Regression Artificial Neural Network (ANN), Pattern Recognition Artificial Neural Network, and rule based filtering were implemented on a dataset obtained from open source SS7 attack simulator [51] to provide a proof of concept. Experiment was performed on a laptop with specifications/ programs given in Table V. In this section fundamental concepts related to implemented techniques along with results are explained.

A. Anomaly Detection

Anomaly detection is the name of finding instances that deviate from expected pattern in a dataset. These instances are called anomalies or outliers [120]. Anomaly detection techniques have been widely used in real time applications to detect unexpected patterns in a system. A straight forward approach of detecting anomalies is to define areas of normal behaviour in the data. Instances which do not belong to this area are called anomalies. Choice of anomaly detection technique depends on multiple factors such as the nature of the available dataset, format of available data (labelled/ unlabelled), and nature of anomalies to be detected. There are three broad categories of machine learning used for anomaly detection[120][121]:

1) Supervised Learning: If the machine is trained on a labelled dataset for both, normal and anomalous instances, it is called supervised learning. A predictive model is built for normal vs anomalous class of the data in training phase. In testing phase, unseen data is compared to both models to determine it belongs to which class [122].

2) Semi-supervised Learning: If the machine is trained on a labelled dataset for only normal class, it is called semi supervised learning. Some anomaly detection techniques are also available which work on the labelling of only anomalous instances. These techniques are less used because it is considered unnatural to assume that training data set covers all possible anomalous instances[121].

3) Unsupervised Learning: If the dataset is unlabelled and it contains greater number of normal instances as compared to anomalous instances, then unsupervised learning can be used. In this technique, training data is not required. machine works on the actual data set to separate anomalies from normal data. If normal instances are not far greater than anomalous instances, it will produce high false alarm rate [121].

Within these broad categories, various methods can be used as per requirements. Various research papers and surveys are available in the literature [120]-[128] to help the user for selection and use of the most relevant technique.

B. K-Means Clustering Algorithm

K means clustering alogorithm is one of the most popular and simple clustering algorithm [129]. It is an unsupervised learning algorithm which is used to partition unlabelled data into clusters. It needs no training data, and computations are performed on actual dataset to make clusters of data points with similar features. This algorithm does not predict next data point, rather each data point is assigned to one of the clusters. Inputs to algorithm are:

- Unlabelled dataset.
- Number of clusters (K) need to be formed.
- Initial position (centroid) for each cluster.

Algorithm used for this experiment checks distance of each data point from all cluster centroids iteratively with the defined features from dataset and assigns it to the nearest cluster. Its working can be explained as under [130].

Step 1:

- We used a dataset of 35640 points e.g. $x_1, x_2, x_3 \ldots\ldots x_n$. This dataset along with a positive integer K (two in our case) was supplied to the algorithm where K represents the number of clusters need to be formed. Initial position of 2 centroids was chosen randomly.

Step 2:

- In step 2, algorithm calculates the distance of each data point from each centroid and assigns it to the nearest centroid. The distance between data points and centroids can be calculated by different methods but Euclidean distance is the most popular method. In our implemented K-means clustering algorithm, Euclidean distance is used to calculate the distances between data points and centroids. It is calculated by the following formula [131]:

$$d(a,b) = \sqrt{(b_1 - a_1)^2 + (b_2 - a_2)^2 + \ldots\ldots + (b_n - a_n)^2} \quad (1)$$

$$d(a,b) = d(b,a) = \sqrt{\sum_{i=1}^{n} (b - a)^2} \quad (2)$$

Step 3:

- Let the set of data points assigned to each i^{th} cluster centroid be S_i. Centroid c_i is recomputed by taking mean of all data points assigned to that centroid by following formula:

$$c_i = \frac{\sum_{x_i \in s_i} (x_i)}{|s_i|} \quad (3)$$

Step 4:

- Algorithm goes back to step 2 and reassigns the data points to the newly computed centroids and then recomputes the centroids. The iterations go on till it finds stopping criteria.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

C. Artificial Neural Networks (ANN)

The idea of ANN has been derived from biological neural networks. The purpose of ANN is to replicate the functionality of biological neural system in learning, correlating, and improving with experience while solving complex problems. ANN structure consists of multiple interconnected units for data processing. These interconnected units are called artificial neurons or nodes[133]. While designing ANNs, the goal of designer is to adopt features of biological systems like learning with experience, fault tolerance, parallel processing of the data, adaptivity, and ability to generalize [134].

1) Structure of ANN: As already described, ANNs consist of neurons. Input neurons take input data, process it, and forward results to the next layer [134]. Next layer does not get input directly from the user program, rather it takes result from previous layer of neurons. The output is given by the output layer. Layers between input layer and output layer are called hidden layers. At each neuron, inputs are multiplied by a weight and then a mathematical function computes its activation based on a threshold value set by the user. Multiple neurons are grouped together to form ANN.

If we take mathematical function as summation, a neuron computes weighted sum of all input signals and generates an output y based on threshold u [133].

$$y = \theta(\sum_{j=1}^{n} w_j x_j - u) \tag{4}$$

- x_j = Variable on j_{th} input
- w_j = Variable on j_{th} Weight
- θ = Unit step function at 0
- u = Threshold value for activation of neuron

Based on network architecture, ANNs are divided into two main categories.

2) Recurrent or Feedback Networks: These networks have a memory of last state of network and are considered as dynamic networks. They update their state continuously based on their previous state until they achieve an equilibrium state. When input is given, they compute output. The input is modified with the output feedback and neuron enters into a new state. Neurons have bi-directional connections between them because of loops in the network.

3) Feed-Forward Networks: In feed forward networks, neurons have unidirectional connections between them i.e from input to output and they can be considered as static networks. Output of one layer only affects the next layer but not the same layer. They are memory less networks as their output is independent of previous network state. Persistence of previous state to draw meaningful conclusion is very important while dealing with complex problems. Non persistence of previous state seems to be a major drawback of these networks.

D. Template for Rule Based Filtering

A proposed template which was implemented in python is shown in Fig. 23. Simple rules in form of if-else statements were defined and implemented. This template can be extended to include other features and other type of MAP messages as per available dataset. Due to limitations of data set received from simulator (limited number of features), machine learning using other features block in Fig. 23 could not be used in the experiment. However, in real SS7 data, it can be used.

E. Implementation Methodology

Open source SS7 attack simulator [51] was used to generate the SS7 traffic. The simulator is built on open source JSS7 stack by Restcomm [135]. In addition to the JSS7 GUI and Core Modes, it is built with following additional modes:

1) Simple Mode: It supports following attacks:

- Location tracking using Any Time Interrogation message (location:ati).
- Location tracking using Provide Subscriber Information message (location:psi).
- Intercepting SMS by stealing subscribers (intercept:sms).

2) Complex Mode: In complex mode, simulator is built to generate normal and attack data for a set of subscribers which are passed as input string to the simulator.

The details of the simulator and its working can be seen in [48]-[50] Simulator was run in simple (SMS intercept) and complex modes to generate a dataset that contained both normal and attack packets. This data was captured on lo interface of Wireshark.

In case of real SS7 traffic, a network provider has a huge amount of data for all subscribers. It is considered difficult to process and use such a huge amount of data for anomaly detection collectively for all subscribers. Concept of anomaly detection for only one user given in [48]-[50] was followed. Data needed to be pre-processed before using it for detection of anomalies. Following important and relevant data attributes were extracted from (Wireshark) pcap file into a csv file with a terminal command:

@ rootkali tshark -r input.pcap -Y gsm_map -T fields -e all required fields > output.csv.

Following fields were extracted:

- Time of the MAP message.
- Destination address (dpc).
- Source address (opc).
- Length of MAP message.
- Type of MAP message.
- Subscriber IMSI.
- SCCP details.
- Area from which message generation is simulated
- Location Area Code.

This dataset contained data for a set of subscribers. With simple grep command from terminal, all data of one particular subscriber was separated from this dataset using IMSI of a

TABLE V
SYSTEM SPECIFICATIONS ON WHICH PROOF OF CONCEPT PERFORMED

System/ Program	Specifications
Operating system	Open source operating system Kali Linux
Processor	Intel(R) Core(TM) i5 2410M CPU @ 2.30 GHz
RAM	8.00 GB
Hard Disk	500 GB
MATLAB	9.3 Release R2017 a (For ANNs)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

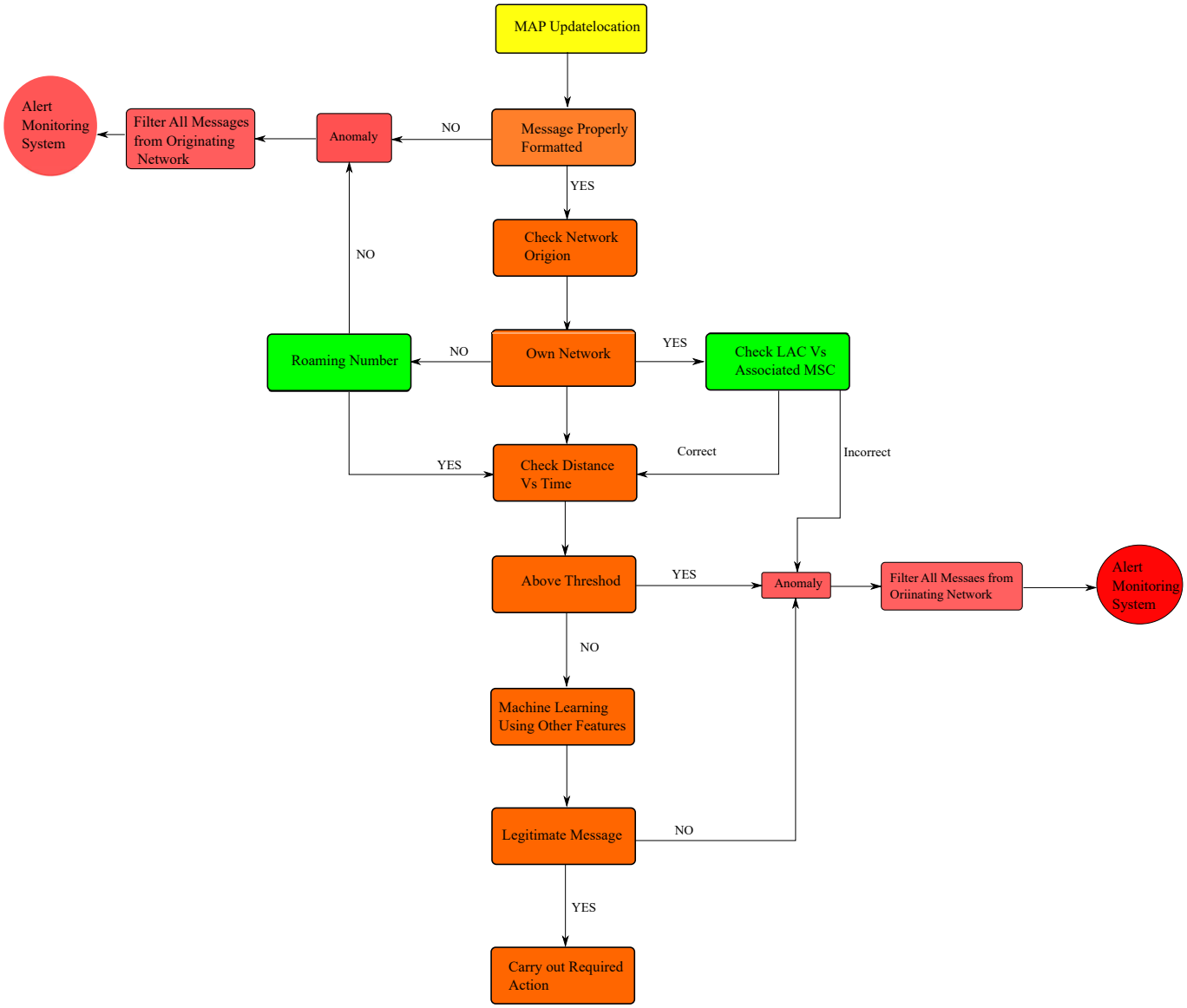


Fig. 23. Template for rule based filtering

Fig. 24. Conversion of a user movements between LACs into distance - Normal user profile indicates the places where a user normally moves i.e., goes to office, goes to a vacation. Any SS7 message coming from LACs which are inside normal user profile, are converted into normal distance. If any message comes from a LAC which is outside normal user profile, it will be converted into abnormal distance, and indicates an attack because the user is not expected to go in that area.

subscriber. The separated data contained normal and attack traffic for a particular subscriber. Again grep command was used to separate MAP Update Location messages for that subscriber. Open source python scripts are also available to preprocess the data for machine learning [136]. The received dataset contained normal and attack MAP Update Location messages for a single subscriber. Different features of this dataset have been used for machine learning as under:

- Time difference between MAP update location messages is used to check distance travelled vs time taken. Time of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

the movement of subscriber is also used in training the neural network.

- Local Area Codes (LACs) is used to model normal behaviour of the user assuming that user do not travel out of a particular area in normal circumstances. Simulator provides only a limited set of LACs. Due to which, this feature is not directly used for machine learning. Here, movements between different LACs is used to define normal behaviour of the subscriber. However in real time data, this feature can be very useful for modelling subscriber's movements.
- Length of the MAP messages in bytes and format of received message is used to check malicious messages. This feature is used on the assumption that the attacker crafts attack packets which slightly vary from original format/size[48] of MAP update message used by the service provider.
- Correlation of MSC addresses vs corresponding LACs can be used for detection of an attack packet received from own network as it will be easy to check received message MSC address and present LAC of the user. Simulator provides a very limited set of these addresses due to which this feature is not used with this data set. In real time, if a network operator can compare LAC & MSC pair received, with those actually implemented within a network, it will give a very good indication of an attack assuming an attacker does not know addresses of MSCs.

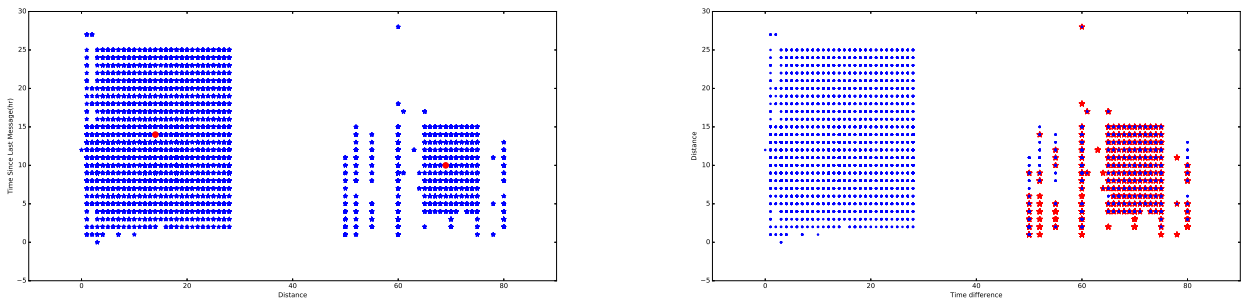
Dataset received from the simulator contains only a limited number of LACs; where a user moves, and from where attack packets are created. These limited LACs cannot be used for defining the user profile to detect anomalies directly. However movements of a selected user from one LAC to another LAC are converted into distance travelled. Distance is used to compare with time elapsed since last message as one of the features.

Let us say our selected subscriber normally moves in the LAC_1 through LAC_n as shown in Fig. 24. The distance between LACs in which a user normally moves is kept less than X km where $X = x_1, x_2, x_3 \ldots\ldots x_n$.
The user moves from LAC_1 to LAC_2 and covers distances x_{12}
Distance$(LAC_1, LAC_2) = x_{12}$
User moves from LAC_2 to LAC_3 and covers distances x_{23}
Distance$(LAC_2, LAC_3) = x_{23}$
The user moves from LAC_1 to LAC_3 and covers distances x_{13}
Distance$(LAC_1, LAC_3) = x_{13}$
.
.
.
.
Distance$(LAC_1, LAC_n) = x_{1n}$

Case 1

We consider that subscriber normally moves in normal user profile. When subscriber moves from one area (LAC) to another area (LAC), her position in the network is updated through MAP Update Location message. Distance between LACs outside of the user profile is kept more than y km in following way [48]-[50]:
Distance between any LAC in a user normal profile and an unknown LAC outside the user normal profile is equal in both directions (from normal profile to a new area and back from the new area to normal profile) and it is greater than distance between any LAC within the user normal profile.
Distance$(LAC_{1,2,3\ldots.n}, LAC_{unknown})$
$= Distance(LAC_{unknown}, LAC_{1,2,3\ldots\ldots n}) = y > X$

Problem in This Method: We assume a user was in LAC_1 and this LAC was registered with the network as the user position. The user was attacked and a malicious packet came from $LAC_{unknown}$. Movement of the user from LAC_1 to $LAC_{unknown}$ will be converted into distance y_1 km ($y_1 > X$). This deviates from normal distance pattern of the user (i.e $x_1 - x_n km$). If we use this feature in any algorithm it can be detected as an anomaly. The trouble starts when a legitimate user moves to LAC_2 and updates her position via MAP Update Location message. The distance from $LAC_{unknown}$ to LAC_2 will be translated into $y_2 (y_2 > X)$. This will be almost same distance as y_1. Though this is a legitimate message but it will again be considered an anomaly by the algorithm. Another issue in this method is that if the user moves away from normal profile area into a new area, it will again be considered an anomaly.



(a) k-means clustering

(b) Rule based filtering

Fig. 25. Distance from user normal profile is kept equal in both directions

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

Proposed Solution(Case 2)

Let us consider distance from a user normal profile and an unknown LAC outside the user normal profile is not equal in both directions. Distance from normal profile to a new area is kept greater than distance between any LAC within the user normal profile but distance from an area outside the user normal profile back to the user profile is kept equal to normal distance used between LACs inside the user profile.

$\text{Distance}(LAC_{1,2,3....n}, LAC_{unknown})$
$\neq Distance(LAC_{unknown}, LAC_{1,2,3.....n})$
$\text{Distance}(LAC_{1,2,3....n}, LAC_{unknown}) = y(y > X)$
$\text{Distance}(LAC_{unknown}, LAC_{1,2,3.....n}) = X$

In above scenario, when a user moves to LAC_2 the distance will be translated to normal distance and it will not be considered an anomaly. Again the same problem exists here, if user moves away from normal profile area into a new area it will again be considered an anomaly.

F. Results

After obtaining a dataset of 35640 sample messages which contained 2248 malicious packets, following features were selected for machine learning as recommended by [48]-[50]:

- Distance travelled by a user.
- Time taken to cover the distance.
- Format of message/ Byte length. This feature can only be used if an attacker sends messages which has higher or lower number of bytes than a normal message of the same type or if message is not properly formatted. If message is properly formatted then this feature will give no indication of an attack or malicious intent.
- Originator address (OPC). MAP update location message can be originated from own network or from a roaming partner. It can be filtered on the basis of OPC if it is other than own network or a roaming partner.
- Frequency of MAP Update messages.

In case 1, K-Means Clustering Algorithm detected 4390 packets as anomalies. All the actual malicious packets were detected correctly and 2142 false positives were generated. These 4390 packets were assigned same cluster as shown in Fig. 25a. As explained in case 1, the distance was almost same for two packets i.e the attack packet and the immediate packet after the attack packet. Attack packet was sent by the attacker from $LAC_{unknown}$. It was translated into abnormal distance. However, when the user moved to a new location and her location was updated, again distance from $LAC_{unknown}$ to the user normal profile was translated to abnormal distance. The algorithm assigned same cluster to both the packets as shown in Fig. 25a, based on the distance involved. Cluster on right side of Fig. 25a show both types of packets were assigned same cluster. In case 2, K-Means Clustering algorithm detected 2987 packets as anomalies. All the actual anomalies were detected correctly and 739 false positives were generated as compared to 2142 anomalies in case 1. The reduction in false positives observed because in case 2 distance for two packets, attack packet and immediate (legitimate) packet after attack packet was not same. False positives in this case were due to other features of the data set being used.

Rule based filtering detected 3365 packets as anomalies with 1117 false positives in both the cases because of nature of artificial data. Two dimensional plots of K-means clustering and Rule based filtering for case 1 are shown in Fig. 25a and 25b. In Fig. 25b red dots indicate attack packets and blue dots indicate normal packets. In rule based filtering, in cluster on right side of Fig. 25b, two packets i.e the attack packet and the immediate packet after the attack packet can be seen with red and blue dots respectively. The attack packet sent by the attacker was detected as attack packet and is shown in red colour and immediate legitimate packet after attack packet due to user movement was detected as normal packet. Rule based filtering could not detect attack packets which were sent within the user normal profile from the attacker.

ANNs were applied on a reduced dataset of 10945 samples due to requirement of labels. Results are summarized in table VI.

From results obtained in table VI, it can be concluded that for real SS7 data, rule based filtering should be implemented for all SS7 MAP messages at first defensive layer. As we have seen, machine learning can also be implemented with a considerable success, at second defensive layer appropriate machine learning algorithm should be applied with carefully chosen features from user data.

Machine learning can be used for detection of all types of anomalies in the SS7 network. It has the potential to detect zero day attacks; however, it may miss some valid attacks and may give more false alarms as compared to rule based filtering.

Rule based filtering can be used for filtering of particular types of messages with greater accuracy as compared to machine learning techniques. It is expected to generate less false alarms as compared to machine learning techniques. There are certain limitations with rule based filtering which include each type of the SS7 message will need a separate rule based template to detect attacks. For designing these templates, greater understanding of internal working of the SS7 network is needed. Moreover, it is not expected to detect zero day attacks.

VII. Future Work

Research on impact of the SS7 vulnerabilities on LTE/4G and 5G networks due to backward compatibility remains an open area of research. Attacks on diameter protocol has been described as an evolution of the SS7-based attacks [13] which needs be further studied to find out the extent of compromise to the users private parameters possible with these attacks.

Development of filtering techniques for MAP SRI and MAP SRI SM messages is an open area of research because these messages are used for legitimate purpose and can be originated from any network. Techniques to detect such malicious messages remain a challenge.

In case of real SS7 traffic, a network provider has a huge amount of data for all subscribers. One of the challenges is to process such a huge data simultaneously for online detection of attacks on the SS7 networks. To process such a huge data feasibility of existing tools/ techniques need to be ascertained. Moreover, development of new tools/ techniques for efficient processing of huge data is also an open challenge.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

TABLE VI
COMPARISON OF RESULTS

	Case1-Equal distance To and From user normal profile				Case 2- Un-Equal distance To and From user normal profile			
	Detection Rate %	False Pos%	False Neg%	True Pos %	Detection Rate %	False Pos%	False Neg%	True Pos %
K-Means Clustering	100	49	Nil	51	Results presented in[48]-[50]			
SHESD Algo	100	43	Nil	57	Results presented in [48]-[50]			
K-Means Clustering	100	48.8	Nil	51.2	100	24.75	Nil	75.25
Rule Based Filtering	98.8	33.2	1.2	66.8	98.8	33.2	1.2	66.8
Pattern recog ANN	99.50	29.4	0.50	70.6	99.58	24	0.42	76
Gen Regression ANN	99.75	27.6	0.25	72.4	99.79	33	0.21	77

Access to real data of SS7 remains the main limiting factor for academia due to privacy issues. However, development of a fully virtual SS7 network/ test bed needs to be studied to facilitate future research on this topic.

The SS7 attack simulator can be considered a good initial step towards development of a fully functioning SS7 attack simulator. As a future work its functionality can be extended to include maximum SS7 MAP messages and all publicly disclosed attacks. In this work only one type of MAP message (MAP update location message) was focused keeping in mind the capabilities of simulator. In future work, scope of detection of malicious MAP messages can also be increased to include all types of attack messages. Implementation of more machine learning techniques can also be investigated to check their feasibility. Moreover rule based filtering templates can be defined and implemented for all types of MAP messages which can be exploited by the attackers. In real SS7 data, both techniques (rule based filtering and machine learning) are recommended to be checked simultaneously for determining the accuracy of proposed method.

VIII. CONCLUSION

Telecommunication networks have gained a significant popularity due to various factors. Signalling system is used for management of calls in telecommunication systems. The SS7 was designed in 1970s on the concept of a boundary walled technology. With the passage of time as the boundary walls of the SS7 network expanded, it has become increasingly open to more service providers. This expansion has resulted in increased interfaces and developed certain threats to the privacy of the subscribers. In this paper, methods to enter into the SS7 network have been explained due to lack of inherent security controls. It has been explained in the paper that location tracking of a subscriber is possible at MSC level which can be narrowed down to a smaller area. Possibility of location tracking to a cell level and accurate location tracking has also been explained. Cases for interception, storage and modification of calls and short messages have been described. Possibility to create DoS, sending spam messages and carrying out fraudulent activities by the attackers has been presented. Different options for defenses against exploitation of the SS7 vulnerabilities have been presented. A machine learning based framework to detect anomalies in the SS7 network has been presented and its results have been compared with rule based filtering on simulated SS7 data set.

ACKNOWLEDGEMENT

This research is supported by the Higher Education Commission (HEC), Pakistan through its initiative of National Center for Cyber Security for the affiliated lab National Cyber Security Auditing and Evaluation Lab (NCSAEL), Grant No: 2(1078)/HEC/M&E/2018/707.

REFERENCES

[1] Positive Technologies, 2016. "Primary Security Threats for SS7 Cellular Networks." [Online]. Available: https://www.ptsecurity.com/upload/corporate/ww-en/analytics/SS7-Vulnerabilities-2016-eng.pdf
[2] H. Sengar, D. Wijesekera and S. Jajodia, "MTPSec: Customizable Secure MTP3 Tunnels in the SS7 Network." In 19th International Parallel and Distributed Processing Symposium, Workshop-17, IPDPS, 2005.
[3] 3GPP TS 23.002 version 14.1.0, Release 14, "GSM, UMTS, LTE Network Architecture." May 2017.
[4] D. Kurbatov and V. Kropotov. (2015). "Hacking mobile network via SS7: interception, shadowing and more." [Online] Available: https://hitcon.org/2015/CMT/download/day1-d-r0.pdf
[5] G. Lorenz, T. Moore, G. Manes, J. Hale, and S. Shenoi, "Securing SS7 Telecommunications Networks." IEEE Workshop on Information Assurance and Security, pp.273-278, June 2001.
[6] M. Isomaki, "Security in the Traditional Telecommunications Networks and in the Internet." White Paper, University of Technology, Helsinki, 1999.
[7] B.Welch. "Exploiting the weaknesses of SS7." Network Security, Volume 2017 Issue 1, pp.17-19, January 2017.
[8] H. Mourad. The fall of SS7-How can the critical security controls help? [Online]. Available: https://www.sans.org/reading-room/whitepapers/critical/fall-ss7--critical-security-controls-help-36225
[9] R.L Brewster,"Packet switched networks." ISDN Technology, pp. 32-41. Springer, Dordrecht, 1993.
[10] V. Mayer-Schonberger and M. Strasser, "Closer look at telecom deregulation: The European advantage." Harv. JL & Tech., vol. 12, p. 561, 1998.
[11] "Telecommunications Act of 1996." US government Publication Office, Public Law 104-104 section 301, 104th Congress, 1996.
[12] A. Spies, JF. Wrede, "The New German Telecommunications Act." Mich. Telecomm. & Tech. L. Rev. 1997 Vol 4 Issue 1.
[13] S. P. Rao, I. Oliver, S. Holtmanns, and T. Aura, "We know where you are!" In 8th International Conference on Cyber Conflict (CyCon), pp. 277-293. IEEE, 2016.
[14] Positive Technologies, December 2014. "Signaling System 7 (SS7) Security Report." [Online]. Available: http://www.ptsecurity.com
[15] M. Mouly and M.B. Pautet, "The GSM system for mobile communications." Telecom Publishing, 1992.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

[16] H. Kaaranen, S. Naghian, L. Laitinen, A. Ahtiainen, and V. Niemi, "UMTS Networks: Architecture, Mobility and Services." New York: Wiley, 2001.

[17] ETSI, TS. "136 101 V10. 3.0 (2011-06) LTE.Evolved universal terresterial radio access (E-UTRA)."

[18] Verint Skylock product brochure: [Online]. Available: http://apps.washingtonpost.com/g/page/business/skylock-product-description-2013/1276/

[19] Defentek Infiltrator product brochure: [Online]. Available: https://assets.documentcloud.org/documents/810690/263-defentek-brochure-infilitrator.pdf

[20] S. Gibbs, "US congressman calls for investigation into vulnerability that lets hackers spy on every phone." The Guardian, 2016. [Online]. Available: https://www.theguardian.com/technology/2016/apr/19/ss7-hack-us-congressman-calls-texts-location-snooping

[21] A. Gellman and A. Gellman, "New documents show how the NSA infers relationships based on mobile location data." Washington Post, 2013. [Online]. Available: https://goo.gl/cCmIzn

[22] C. McDaid, "Can They Hear You Now? Hacking Team & SS7 | AdaptiveMobile." Adaptivemobile.com, 2015. [Online]. Available: http://www.adaptivemobile.com/blog/can-they-hear-you-now-hacking-team-ss7

[23] "Positive Technologies - vulnerability assessment, compliance management and threat analysis solutions." Ptsecurity.com. [Online]. Available: https://www.ptsecurity.com/ww-en/

[24] B. Goodwin, "Security flaw exposes billions of mobile phone users to eavesdropping." Computer Weekly, August 14 2015, [Online]. Available http://www.computerweekly.com/news/4500251756/Security-flaw-exposes-billions-of-mobile-phone-users-to-eavesdropping

[25] C. Timberg, "German researchers discover a flaw that could let anyone listen to your cell calls." The Washington Post, December 18 2014, [Online]. Available: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-\your-cell-calls-and-read-your-texts/?utm_term=.de15e5842bff

[26] B. Clark, "Watch hackers hijack WhatsApp and Telegram accounts using known telecom flaw." June 1 2016, [Online]. Available http://thenextweb.com/insider/2016/06/01/watch-hackers-hijack-whatsapp

[27] P1 Security. December 2014. "SS7map: SS7 Networks Exposure." [Online].Available: https://ss7map.p1sec.com/

[28] G. Lorenz, J. Keller, G. Manes, J. HaIe and S. Shenoi. "Public telephone network vulnerabilities." In Database and Application Security XV, pp. 151-164. Springer, Boston, MA, 2002.

[29] C. Xenakis, and L. Merakos. "Security Architecture Standardization and Services in UMTS." Proc. Mobile Venue, pp 585-592, 2002.

[30] H. Sengar, R. Dantu, and D. Wijesekera, "Securing VoIP and PSTN from integrated signaling network vulnerabilities." 1st IEEE workshop on VoIP Management and Security (VoIP MaSe), Vancouver, Canada, April 2006.

[31] C. Xenakis and L. Merakos, "Security Architecture Standardization and Services in UMTS." Proc. Mobile Venue, pp 585-592, (2002).

[32] H. Sengar, R. Dantu, D. Wijesekera, and S. Jajodia. "SS7 over IP: Signaling internetworking vulnerabilities." IEEE Network 20 (6), pp. 32-41, November 2006.

[33] V. Chandola, A. Banerjee, V. Kumar, "Anomaly detection: A survey." ACM computing surveys (CSUR)41(3), July 2009.

[34] P. Langlois, "SCTPscan-Finding entry points to SS7 networks & telecommunication backbones." In BlackHat Convention (BH), Europe 2007.

[35] "Black Hat", [Online]. Available: http://blackhat.com/

[36] T. Engel, "Locating Mobile Phones using Signaling System#7." In 25th Chaos Communication Congress 25C3 2008, http://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf

[37] K. Kotapati, "Assessing security of mobile telecommunication networks." (2008).

[38] K. Kotapati, P. Liu, and T. F. Porta. "Evaluating MAPSec by marking attack graphs." Wireless Networks 15(8) pp 1042-1058, Springer, 2009.

[39] J. Lingling and M. Hong, "New Trends of Attack and Prevention Technologies in Telecommunication." In Information Technology and Applications (IFITA'09) 1, pp. 80-82. IEEE, 2009.

[40] A. Xinyuan, J. Chen, Y. Liu, X. Wei, and T. Xu, "A defense method based on improved MTP3 message discrimination in SS7 network." In Natural Computation (ICNC), Seventh International Conference (2), pp. 711-715. IEEE, 2011.

[41] S. Mjθlsnes and J. K Tsay, "Computational security analysis of the UMTS and LTE authentication and key agreement protocols." 6th International Conference on Mathematical Methods, Models and Architecture for Computer Network Security(MMM-ACNS 2012), pp. 65-76, Springer, 2012.

[42] A.De Oliveira et al. "Worldwide attacks on SS7 network' Hackito Ergo Summit (2014)." http://2014.hackitoergosum.org/slides/day3_Worldwide_attacks_on_SS7_\network_P1security_Hackito_2014.pdf

[43] "Hackito Ergo Sum 2014 | Hacker Community for Free Security Research." 2018. [Online]. Available: http://2014.hackitoergosum.org/

[44] K.Nohl (SR Labs), "Mobile self-defense' 31st Chaos Communication Congress 31C3." (2014).

[45] "Chaos Computer Club", Ccc.de. [Online]. Available: https://www.https://www.ccc.de/en/home

[46] T. Engel (Sternraute), "SS7: Locate. Track. Manipulate", 31st Chaos Communication Congress 31C3 (2014), http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

[47] S.P Rao, "Analysis and Mitigation of Recent Attacks on Mobile Communication Backend." Master's thesis, University of Tartu, 2015.

[48] K. Jensen. "Improving SS7 Security Using Machine Learning Techniques." Master's thesis, Norwegian University of Science and Technology, 2016.

[49] K. Jensen, T.Van Do, H.T Nguyen, A. Arnes, "Better protection of SS7 using machine learning techniques." In 6th International Conference on IT Convergence and Security (ICITCS) (2016).

[50] K. Jensen, T.Van Do, H.T Nguyen, A. Arnes, "A big data analytics approach to combat telecommunication vulnerabilities" Cluster Computing 20(3), pp.2363-2374, 2017

[51] "SS7 Attack Simulator based on RestComm's jss7." [Online]. Available: https://github.com/polarking/jss7-attack-simulator

[52] S. Holtmanns, S. P. Rao, and I. Oliver, "User location tracking attacks for LTE networks using the interworking functionality." In 2016 IFIP Networking Conference (IFIP Networking) and Workshops, pp. 315-322, May 2016.

[53] M. Hamdi et al, "Voice Service Interworking for PSTN and IP Networks." IEEE Commun. Mag, pp. 104-11,1999.

[54] M. Savadatti and D. Sharma, "SS7 Network and Its Vulnerabilities: An Elementary Review." Imperial Journal of Interdisciplinary Research (IJIR)3(3), pp. 912-916, 2017.

[55] S. Puzankov, "Stealthy SS7 Attacks", Journal of ICT Standardization 5(1), pp. 39-52, 2017.

[56] N. Andrews, "CAN I GET YOUR DIGITS? ILLEGAL ACQUISITION OF WIRELESS PHONE NUMBERS FOR SIM-SWAP ATTACKS AND WIRELESS PROVIDER LIABILITY, 16 Nw. J. Tech. & Intell. Prop. 79 (2018)." https://scholarlycommons.law.northwestern.edu/njtip/vol16/iss2/2

[57] C. Liu, X.Ji, J. Wu, et al, "A proactive defense mechanism for mobile communication user data." Sci China Inf Sci, 2018, 61(10): 109303, https://doi.org/10.1007/s11432-017-9428-6

[58] L. Abdelrazek and M. A Azer. "SigPloit: A New Signaling Exploitation Framework." In Tenth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 481-486. IEEE, 2018.

[59] T. Qasim, M. Hanif Durad, A. Khan, F. Nazir, and T. Qasim. "Detection of signaling system 7 attack in network function virtualization using machine learning." In fiteenth International Bhurban Conference on Applied Sciences and Technology (IBCAST), pp. 484-488. IEEE, 2018.

[60] T.M Aung,K.H Myint,and N.N Hla. "A Data Confidentiality Approach to SMS on Android." In International Conference on Intelligent Computing & Optimization, pp. 505-514. Springer, Cham, 2018.

[61] Prof. J. Kulubi, "Glossary of terms & standards used in telecommunication systems." [Online]. Available: http://eti2506.elimu.net/Glossary/Glossary_Telecom.html

[62] O. Kong Chung, "SS7 OPNET simulation Signaling System No.7, (SS7) network interfaces." Master's Thesis, Naval Postgraduate School, California, 2000.

[63] J. Van Bosse and F. Devetak, "Signaling in telecommunication networks." Hoboken, N.J.: Wiley-Interscience, 2007.

[64] J. Van Bosse and F. Devetak, 'Signaling in telecommunication networks'. Hoboken, N.J: Wiley-Interscience, 2007, Chapter7 pp (157-166).

[65] Performance Technologies, "Tutorials on Signaling Sytem 7 (SS7)." [Online]. Available: https://www.net.t-labs.tu-berlin.de/teaching/computer_networking/documents/ss7_tutorial_pt.pdf

[66] H. Rafik and M. T. El-Hadidi, "Structured Approach for Planning Signalling System No. 7 Networks." In Second IEEE symposium on Computers and Communications, pp. 109-113, 1997.

[67] CAP, CAMEL Application Part. "TS-3GA-29.078 (Rel4) v4. 4.0 Customised Applications for Mobile network Enhanced Logic (CAMEL); CAMEL Application Part (CAP) specification." (2002).

[68] GSMA Intelligence, white paper on "Mobile network technology lifecycle:the future of 2G networks." [Online]. Available: https://www.gsmaintelligence.com/research/?file=5f6d4734e6ae137fba76acf6cc7b1d88&download

[69] N. Mitra, S.D. Usikin "Relationship of SS7 protocol architecture to the OS1 Reference Model." IEEE Network Magazine Jan. 1991.

[70] "Dialogic DSI SS7 Stack | EiconWorks.com." [Online]. Available: http://www.eiconworks.com/DSI-SS7-Stack.asp

[71] A. R. Modarressi, R. A. Skoog, "Overview of Signaling System No. 7 and Its Role in the Evolving Information Age Network." Proc. IEEE, pp. 590-606, 1992.

[72] 3GPP TS 33.204, version 8.0.0, Release 8, "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G Security;Network Domain Security (NDS); Transaction Capabilities Application Part (TCAP) User Security, Release 8."

[73] 3GPP TS 29.002, Release 13, "Mobile Application Part (MAP) Specification." 2015. http://www.3gpp.org/DynaReport/29002.htm

[74] 3GPP TS 33.200, version 4.2.0, Release 4,"Universal Mobile Telecommunications System (UMTS; Network Domain Security - MAP."

[75] 3GPP TS 33.200, Version 5.0.0, Release 5, "Technical Specification Group Services and System Aspects, 3G Security; Network Domain Security; MAP application layer security."

[76] 3GPP TS 23.002, Release 13, "Network architecture" September 2015.

[77] ICT Workshop by Huawei, "GSM Core Network Overview". [Online]. Available http://technocratseservices.blogspot.com/2013/09/gsm-core-network-overview.html

[78] B. Gabelgaard, "The (GSM) HLR-advantages and challenge." In Third Annual Universal Personal Communications conference, 1994.

[79] 3GPP TS 23.040, Release 13, "Technical realization of the Short Message Service (SMS)."

[80] 3GPP TR 23.039, "Interface Protocols for the Connection of Short Message Service Centers (SMSCs) to Short Message Entities (SMEs)."

[81] 3GPP, TS 22.016, "Technical Specification Group Services and System Aspects; International Mobile station Equipment Identities (IMEI)."

[82] 3GPP, TS 23.003, "Technical Specification Group Core Network and Terminals; Numbering, addressing and identification (Release 9)".

[83] P. Langlois, "Getting in the SS7 kingdom: hard technology and disturbingly easy hacks to get entry points in the walled garden." 2010, [Online]. Available: http://www.hackitoergosum.org/2010/HES2010-planglois-Attacking-SS7.pdf

[84] R. Stewart, "Stream Control Transmission Protocol," RFC Editor, 2007.

[85] V. Chandrasekhar, J. G. Andrews, and A. Gatherer, "Femtocell networks:a survey." IEEE Communications Magazine 46(9), pp. 59-67, 2008.

[86] T. Moore, T. Kosloff, J. Keller, G. Manes, and S. Shenoi. Signaling system 7 network security. In 45th Midwest Symposium on Circuits and Systems, IEEE, August 4-7, 2002.

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

[88] L. Ong et. al, "Framework Architecture for Signaling Transport." RFC 2719, IETF, 1999.

[89] R. Stewart, "Stream Control Transmission Protocol." RFC Editor, 2007.

[90] "SCTPscan: SCTP Network And Port Scanner." P1 Security, [Online]. Available: http://www.p1sec.com/corp/research/tools/sctpscan/

[91] P. Biondi, Scapy Project Home Page, 2015. [Online]. Available: http://www.secdev.org/projects/scapy/

[92] 3GPP, 3GPP TS 23.066, "Support of Mobile Number Portability (MNP); Technical realization; Stage 2."

[93] P. Chandra, "Bulletproof wireless security: GSM, UMTS, 802.11, and adhoc security." Elsevier, 2005.

[94] Y. B Lin, and M. H Tsai, "Eavesdropping Through Mobile Phone." IEEE Transaction on Vehicular Technology 56(6), pp. 3596-3600, 2007.

[95] G. Peersman, S. Cvetkovic, P. Griffiths, and H. Spear, "The global system for mobile communications short message service." IEEE Personal Communications 7(3), pp 15-23, 2000.

[96] 3GPP TS 23.078, "Customized Applications for Mobile network Enhanced Logic (CAMEL)."

[97] C. Pudney, "3GPP TSG-SA WG2 meeting #22, 2002: Liaison Statement on Restoration of R'96 Any Time Interrogation functionality." 3rd Generation Partnership Project.

[98] 3GPP TS 04.31, "Location Services (LCS); Mobile Station (MS)-Serving Mobile Location Centre (SMLC) Radio Resource LCS Protocol (RRLP)."

[99] T. Oza, "LCS Capable GSM Network." Master's thesis, Uppsala University, 2015.

[100] Station, Mobile. "Serving Mobile Location Centre (SMLC) Radio Resource LCS Protocol (RRLP)" http://www.3GPP.org (2009)

[101] Shodanhq.com, SHODAN - Computer Search Engine.

[102] "Unwired Labs," [Online]. Available: http://unwiredlabs.com/api

[103] S. P. Rao, S. Holtmanns, I. Oliver, and T. Aura, "Unblocking stolen mobile devices using ss7-map vulnerabilities: Exploiting the relationship between IMEI and IMSI for EIR access." In Trustcom/BigDataSE/ISPA 1, pp. 1171-1176, IEEE, 2015.

[104] Bellcore: Bell Communications Research Specification of Signaling System Number 7, GR-246-CORE, T1.111.4, Issue 3, December 1998.

[105] SR Labs, "SnoopSnitch," Security Research Lab.

[106] S. Udar and R. Borgaonkar, "Understanding IMSI Privacy." In Vortrag Auf Der Konferenz, Blackhat USA, 2014.

[107] 3GPP, TR 23.840, Release 7 "Study into routing of MT-SMs via the HPLMN. 2007, http://www.3gpp.org/DynaReport/23840.htm

[108] F. Oneglia and T. Baritaud, "CCS 7 Networks Dependability Studies: Phase 2 Deliverable 2." Technical Report Annex A - Protocol Analysis in Access Control, June 1998.

[109] C. Groves, M. Pantaleo, T. Anderson, and T. Taylor, "RFC 3525 :Gateway Control Protocol Version 1." IETF Network Working Group, June 2003.

[110] L. Ong, I. Rytina, M. Garcia, H. Schwarzbauer, L. Coene, H. Lin, I. Juhasz, M. Holdrege, and C. Sharp, "RFC 2719 : Framework Architecture for Signaling Transport." IETF NetworkWorking Group, October 1999.

[111] G. Sidebottom, K. Morneault, and J. Pastor-Balbas, "RFC 3332 : Signaling System 7 (SS7) Message Transfer Part 3 (MTP3-User Adaptation Layer (M3UA)." IETF Network Working Group, September 2002.

[112] K. Chung, "Prototyping and evaluation of TCAPsec." Degree Project, Karlstad University, 2007.

[113] D. Rupprecht,A. Dabrowski, T. Holz, E. Weippl, and C. Popper, "On security research towards future mobile network generations." IEEE Communications Surveys & Tutorials 20 (3), pp: 2518-2542, IEEE, 2018.

[114] Tony Murphy, "Major security flaw in SS7-how SMS Home Routing can plug the gap." Online Blog available at: http://www.cellusys.com/2016/04/25/major-security-flaw-in-ss7-how-sms-home-routing-can-plug-the-gap/

[115] V. Kapoor, V. Sonny Abraham, and R. Singh, "Elliptic curve cryptography." ACM Ubiquity 9(20), pp: 20-26, 2008.

[116] R. Housley, In "Public Key Infrastructure (PKI)." John Wiley & Sons, Inc.; 2004, [Online]. Available: http://dx.doi.org/10.1002/047148296X.tie149

[117] Z. Zhang et al, "An Overview of Virtual Private Network (VPN): IP VPN and Optical VPN." Photonic Network Communication 7(3), pp. 213-225, 2004.

[118] G. Huston, G.S Kent Michaelson," Certification Authority (CA) Key Rollover in the Resource Public Key Infrastructure (RPKI)." BCP 174, RFC 6489, February; 2012.

[119] F. Sabahi and A. Movaghar, "Intrusion Detection: A Survey," In Third International Conference on Systems and Networks Communications, pp. 23-26, Sliema, 2008.

[120] V. Chandola, A. Banerjee and V. Kumar, "Anomaly detection: A survey." ACM computing surveys (CSUR) 41(3), p:15, 2009.

[121] A. L Buczak, and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection." IEEE Communications Surveys & Tutorials, 18(2), pp.1153-1176, 2016.

[122] T.T Nguyen and G. Armitage, "A survey of techniques for internet traffic classification using machine learning." IEEE Communications Surveys & Tutorials, 10(4), pp.56-76, 2008.

[123] G.E Batista, R.C Prati and M.C Monard, "A study of the behavior of several methods for balancing machine learning training data." ACM SIGKDD explorations newsletter, 6(1), pp.20-29, 2004.

[124] T. Hofmann, "Unsupervised learning by probabilistic latent semantic analysis." Machine Learning, 42(1-2), pp.177-196, 2001.

[125] J. Dougherty, R. Kohavi, and M. Sahami, "Supervised and unsupervised discretization of continuous features". In Machine Learning Proceedings, pp. 194-202, Morgan Kaufmann, 1995.

[126] S.B Kotsiantis, I. Zaharakis, and P. Pintelas,"Supervised machine learning: A review of classification techniques." Emerging Artificial Intelligence Applications in computer engineering 160, pp.3-24, 2007.

[127] A. Shabtai, R. Moskovitch, Y. Elovici, and C. Glezer,"Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey." Information Security Technical Report 14(1), pp.16-29, 2009.

[128] N. Williams, S. Zander and G. Armitage, "A preliminary performance comparison of five machine learning algorithms for practical IP traffic flow classification" ACM SIGCOMM Computer Communication Review 36(5), pp.5-16, 2006.
[129] P. Berkhin, "A survey of clustering data mining techniques." Grouping Multidimensional Data, pp. 25-71, Springer, Berlin, Heidelberg,2006.
[130] A. Trevino, "Introduction to K-means Clustering" Online blog. Avaialable: https://www.datascience.com/blog/k-means-clustering?
[131] Euclidean distance, Wikipedia [Online]. Available: https://en.wikipedia.org/wiki/Euclidean_distance
[132] corvasto/Simple-k-Means-Clustering-Python, https://github.com/corvasto/Simple-k-Means-Clustering-Python
[133] I. A Basheer and M. Hajmeer, "Artificial neural networks: fundamentals, computing, design, and application." Journal of microbiological methods 43(1),pp. 3-31, 2000.
[134] A.K Jain, J. Mao and K.M Mohiuddin," Artificial neural networks: A tutorial." Computer 29(3), pp.31-44, 1996.
[135] Restcomm, "jss7 GitHub Repository." 2015, [Online]. Available: https://github.com/Mobicents/jss7/
[136] K. Jensen, "SS7 Preproessing GitHub Repository." 2016, [Online]. Available: https://github.com/polarking/ss7-preprocessing
[137] Vacca, John R. Computer and information security handbook. 2012. Chapter 17

Kaleem Ullah (kaleem_7198@hotmail.com) did his B.E Electronics from PNEC, National University of Sciences and Technology, Pakistan, in 2010. He received his MS Degree in Information Security from MCS, National University of Sciences and Technology, Pakistan, in 2018. He was awarded President's Gold Medal for securing first position in Master degree. His research interests include mobile and wireless communication, Big Data Analysis, Artificial Intelligence, IoT, Software Defined Networking and Information Security.

Imran Rashid (irashid@mcs.edu.pk) did his B.E. in Electrical (Telecomm) Engineering from National University of Sciences and Technology, Pakistan, in 1999. He received his M.Sc. degree in Telecomm Engineering (Optical Communication) from D.T.U Denmark in 2004 and his Ph.D. in Mobile Communication from University of Manchester, UK in 2011. He has qualified four EC-Council certifications i.e. Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), EC-Council Certified Security Analyst (ECSA) and EC-Council Certified Incident Handler (ECIH). He is also a Certified EC-Council Instructor (CEI) and has conducted numerous trainings. Currently, he is Chief Instructor (Engineering Wing), MCS at National University of Sciences and Technology, Pakistan. His research interests are Mobile and Wireless Communication, MIMO Systems, Compressed Sensing for MIMO OFDM systems, Massive MIMO Systems, M2M for Mobile systems, Cognitive Radio Networks, Cyber Security and Information Assurance.

Dr. Hammad Afzal (hammad.afzal@mcs.edu.pk) is currently heading "The Center of Data and Text Engineering and Mining" (CoDTeEM) group at NUST. His primary interests are machine learning, text and data mining systems. He completed PhD from School of Computer Science, University of Manchester, UK in Dec, 2009 under supervision of Dr. Goran Nenadic in Text Mining Group. Before PhD, he completed MSc in Advanced Computing Sciences from University of Manchester, UK where he was awarded Program Prize of the year from Department of Computation for acquiring highest grades in MSc courses. He has also been affiliated with Digital Enterprise Research Institute (DERI), National University of Ireland, Galway as a Research Assistant from July, 2009 to Dec, 2009.

Mian Muhammad Waseem Iqbal (waseem.iqbal@mcs.edu.pk) is an academician, researcher, security professional and industry consultant. He did his bachelor's degree in Computer Sciences from Department of Computer Science, University of Peshawar in 2008. He achieved merit based scholarship throughout his bachelor's degree. He completed his Masters in Information Security from Military College of Signals-NUST in 2012. He was inducted as Lecturer at Department of Information Security (NUST) in May 2012. In Feb 2015 he was promoted as Assistant Professor. Currently he is enrolled in PhD program and is in research phase. His professional services include, but not limited to Industry Consultation, Workshops Organizer/Resource Person, Technical Program Committee member, Conference Chief organizer, Invited speaker and reviewer for several International conferences. He has authored over 35 scientific research articles in prestigious international journals (ISI-Indexed) and conferences. He is principal advisor for more than 8 MS students and 10 UG projects. 8 out 10 UG projects are industry funded projects. Mr. Waseem has conducted more than 15 CEH, CHFI, CSCU and Forensics practical hands on workshops for industry and general public. In recognition of Mr. Waseem services, he was awarded Overall University Best Teacher Award for the year 2014/15.

Dr. Yawar Abbas Bangash (yawar@mcs.edu.pk) received BS degree (2008) in Software engineering from KPK University of Engineering and Technology Peshawar. From 2008 to 2012, he worked in Huawei Organization Pakistan Ltd, Higher Education Commission (HEC) project PERN2, and Baluchistan Education Foundation (BEF) on different positions in networking sector. He won HEC prestigious scholarship "MS leading to PhD" for five years in 2012. In 2014, he received MS degree in Computer Science (Information Security) from Wuhan University of technology, Wuhan, China. In 2017, he received his PhD degree from Huazhong University of Science and Technology (HUST), China. His research interests are: Software Defined Networking, Software Defined Storage, Wireless Sensor Networks, Formal Methods in Software Engineering, AI in Finance, and stock market, Information Security, Cloud Computing, Data Center Networking, IoT, and Security in SDN, WSN and Smart IoT. He has published high quality papers in ISI indexed journals. He also conducted various workshops related to 5G technologies and SDN. In addition, he is supervising 10 MS students and co-supervising 03 PhD students. Currently, he is an Assistant professor in College of Signals, National University of Sciences and Technology, Pakistan.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2020.2971757, IEEE Communications Surveys & Tutorials

Haider Abbas (SM'16) (Haider@mcs.edu.pk) received the M.S. degree in engineering and management of information systems and the Ph.D. degree in information security from KTH, Sweden, in 2006 and 2010, respectively. He is currently heading the National Cyber Security Auditing and Evaluation Lab with MCS-NUST. He is a Cyber Security Professional who took professional trainings and certifications from the Massachusetts Institute of Technology, USA; Stockholm University, Sweden, IBM, and EC- Council. He is an Associate Editor on the editorial board of a number of international journals, including the IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, the Journal of Network and Computer Applications, Electronic Commerce Research, IEEE ACCESS, Neural Computing and Applications and Cluster Computing. He also won many awards and received several research grants for ICT-related projects from various research funding authorities and working on scientific projects in U.S., Europe, Saudi Arabia, and Pakistan. He is the principal advisor for several graduate and doctoral students with the National University of Sciences and Technology, Pakistan, Al-Farabi Kazakh National University, Kazakhstan, the Florida Institute of Technology, USA, and Manchester Metropolitan University, U.K.