

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/339061789>

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

Article in IEEE Communications Surveys & Tutorials · February 2020

DOI: 10.1109/COMST.2020.2971757

CITATIONS

169

READS

8,462

6 authors, including:



Imran Rashid

National University of Sciences and Technology

74 PUBLICATIONS 856 CITATIONS

[SEE PROFILE](#)



Hammad Afzal

National University of Sciences and Technology

85 PUBLICATIONS 1,302 CITATIONS

[SEE PROFILE](#)



Waseem Iqbal

National University of Sciences and Technology

78 PUBLICATIONS 1,050 CITATIONS

[SEE PROFILE](#)



Haider Abbas

National University of Sciences and Technology

169 PUBLICATIONS 5,295 CITATIONS

[SEE PROFILE](#)

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

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

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

I. INTRODUCTION

26 MOBILE telecommunication networks have enjoyed a
27 great popularity from their start due to a number of factors
28 such as low rates, seamless roaming, wide coverage, and
29 portability of cell phones. After the merger of data and voice
30 networks, their popularity increased manifolds. Popularity of
31 social media, user friendly cell phone applications, enhanced
32 processing power, and memory of cell phones are making
33 this technology even more popular. With the passage of time,
34 telecommunication technology has become primary means
35 of communication for personal needs, business requirements,
36 and emergency services. In telecommunication networks, sig-
37 nalling system is used to set up, manage, and tear down a
38 call [1][2]. The SS7 is used to provide mobility management,
39 control billing information, generate user security information,
40 support call establishment/ termination and control access/
41 service authorization [3][4][5]. The SS7 network was designed
42 in 1970s when few national/ multinational telecommunication
43 operators used to provide telecommunication services. These
44 national/ multinational operators had access to core network
45 [1][2]. In this backdrop, no inherent security controls were
46 incorporated in the SS7 core network, and it was designed on
47 the basis of mutual trust between operators [6]. It was assumed
48 that all operators, being national/ multinational corporations,

can be trusted thus assuming the SS7 network as a closed
49 trusted network [7][8].

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

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

A. Limited Research by Academia

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

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

B. Motivation

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

TABLE I
LIST OF ACRONYMS AND CORRESPONDING DEFINITIONS

Acronym	Definition
2/3/4G	2nd/ 3rd/ 4th Generation
3GPP	3rd Generation Partnership Project
AIMSCD	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 Signalling
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

149
150

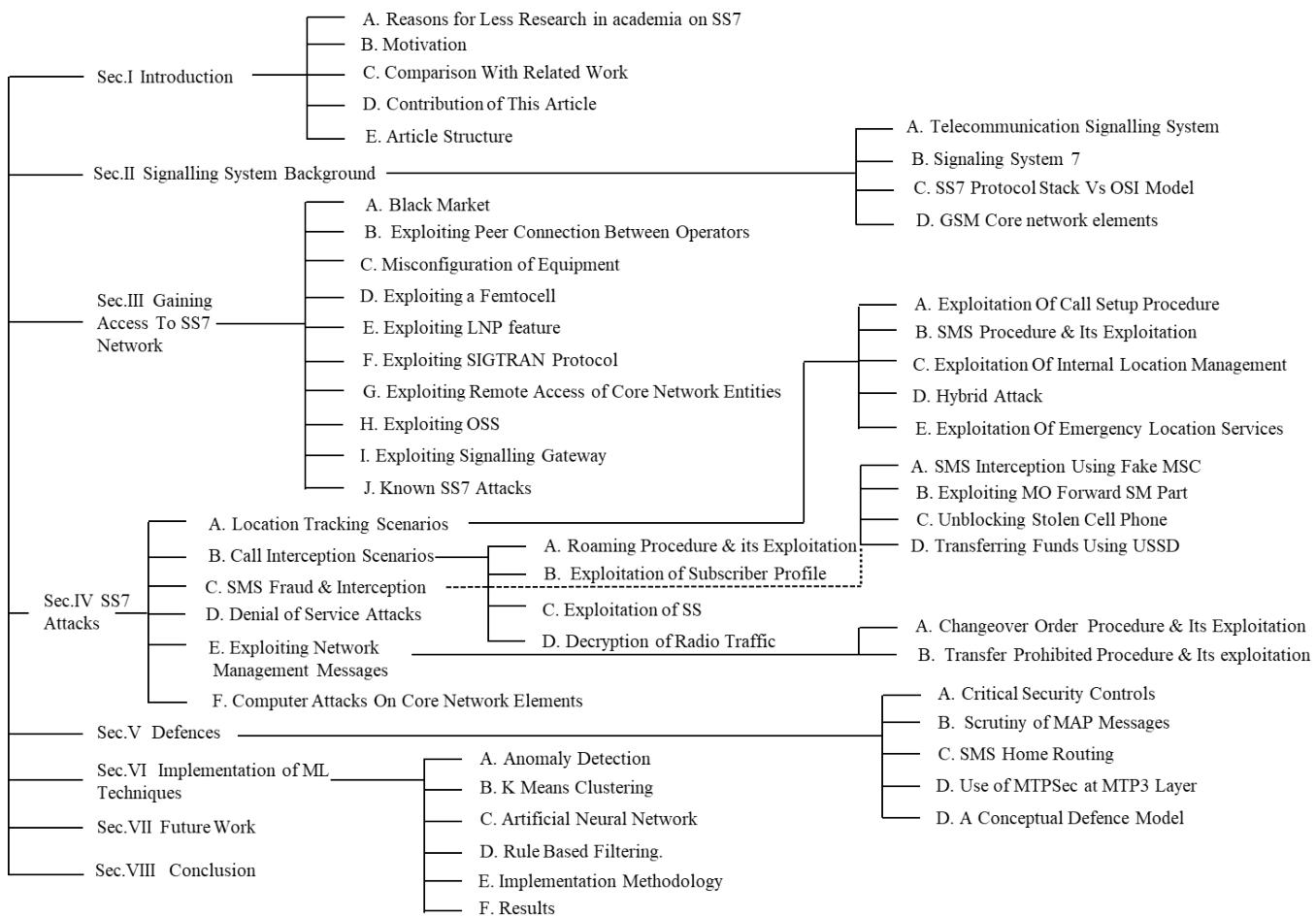


Fig. 1. Taxonomy of the paper.

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

158 C. Comparison with Related Work

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

174 D. Contribution Of This Paper

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

- 178 • A brief note on the background and evolution of telecom-
179 munication signalling systems.
- 180 • An overview of the SS7 protocol stack and GSM core
181 network elements.
- 182 • Possible entry points into the SS7 network.
- 183 • All publicly disclosed location tracking attacks with the
184 detailed method to accomplish these attacks.
- 185 • Call and SMS interception, modification and fraud sce-
186 narios and attack vectors.
- 187 • Possibility of DoS attacks.
- 188 • Detailed defenses against the SS7 attacks.
- 189 • A machine learning based framework to detect anomalies
190 in the SS7 network which is compared with rule based
191 filtering.
- 192 • A conceptual defense model on the basis of an existing
193 model.

TABLE II: Summary of related work

Reference	Year	Summary
G.Lorenz et al[5][28]	2001	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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.

TABLE II: Summary of related work-continued

Positive technologies [14]	2014	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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
Abdelrazeq, Loay, and Marianne A. Azer. [58]	2018	<ul style="list-style-type: none"> - They discussed location tracking and interception of calls/SMS due to vulnerabilities of the SS7.
Qasim, Tooba, M. Hanif Durad, et al. [59]	2018	<p>They discussed the SS7 vulnerabilities in following four categories:</p> <ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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.

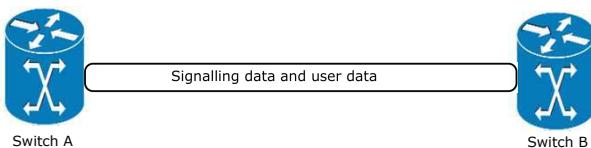


Fig. 2. Channel Associated Signalling.

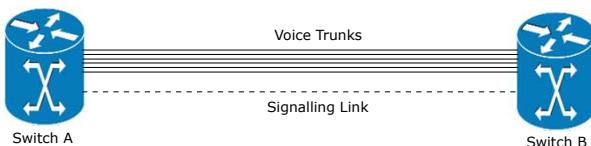


Fig. 3. Common Channel Signalling (associated mode)[61]

194 E. Article Structure

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

207 II. SIGNALLING SYSTEM

208 A. Telecommunication Signalling System

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

219 1) *Channel Associated Signalling (CAS)*: In this type of
220 signalling, same channel is used for transferring control infor-
221 mation (signalling) and actual traffic of the user (voice, data)
222 [63] as shown in Fig. 2. As control information is being sent
223 in the same band which is being used for actual data of the
224 user, it is called in-band signalling. Examples of CAS include
225 Signalling System no 5 (SS5) which was used before 1970.
226 Disadvantages of CAS/ SS5 are as follows:

- 227 • It was inefficient as signalling and actual subscriber's data
228 was competing for transmission.
- 229 • Less bandwidth was available to carry subscriber's data
230 as signalling messages were consuming part of the band-
231 width.
- 232 • It required additional signalling equipment at every node
233 to forward signalling data.

- 234 • Resources of the channel were reserved as soon as
235 signalling started. Even if the recipient was busy or
236 unavailable, the channel remained occupied.
- 237 • Subscribers were able to access signalling messages cre-
238 ating possibility of malicious activities by the subscribers.
239 Due to these disadvantages CAS was replaced with Com-
240 mon Channel Signalling (CCS).

241 2) *Common Channel Signalling*: In CCS, signalling mes-
242 sages are passed on a separate logical path than subscriber's
243 data. It is called common channel signalling because this
244 channel is used commonly to accommodate signalling data
245 of all calls. All signals related to call initiation, management
246 and termination are passed on this channel independent of
247 subscriber's data. The SS6 and the SS7 are examples of CCS
248 [62]. An illustration of CCS is shown in Fig. 3 Advantages of
249 CCS are as follows:

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

261 B. Signalling System No 7

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

- 278 • It enables communication between core network entities
279 for routing of calls.
- 280 • It supports seamless handover of call from one MSC to
281 another MSC when subscriber is moving.
- 282 • It provides roaming facility.
- 283 • It is used to generate billing information.
- 284 • It provides Short Message Service (SMS) initiation and
285 delivery.
- 286 • It provides location tracking facility for emergency ser-
287 vices.
- 288 • It provides toll free (0800) services for government and
289 private organizations [65].

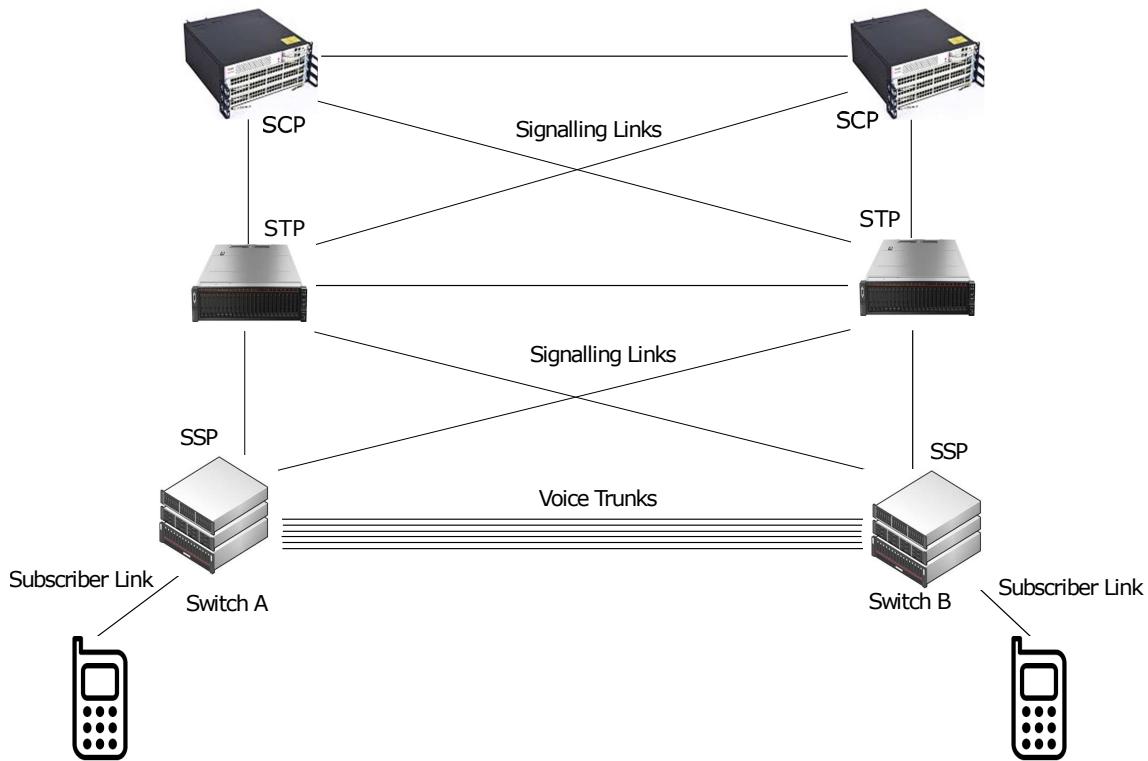


Fig. 4. Basic Building Blocks of the SS7 Core Network [65]

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

292 Few basic elements of the SS7 are described as under:

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

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

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

301 4) *Service Switching Point (SSP)*: The SS7 network
302 consists of three basic signalling points for management of
303 signalling. These signalling points are connected through
304 signalling links as shown in Fig. 4. Primary function of an
305 SSP is to initiate a call when the user dials a number and to
306 terminate a call upon completion. It also gives dialling tone,
307 converts dialled number to the desired code of switch to which
308 it has to be forwarded, and communicates with STPs and SCPs
309 [65].

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

315 6) *Signal Control Points (SCPs)*: SCPS insert intelligence
316 into the SS7 network and provide extra features. It gives
317 instructions to SSPs on how to route calls. Whether to forward
318 the call or not. It runs Customized Application for Mobile

Networks Enhanced Logic (CAMEL) [67] services as well
[46].

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

C. SS7 Protocol Stack Vs OSI Model

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

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

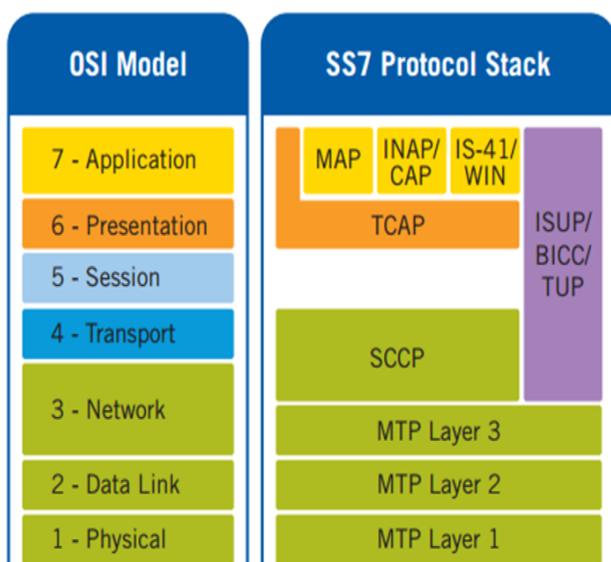


Fig. 5. A Comparison of SS7 protocol stack vs OSI protocol stack [70]

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

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

360 3) *Telephone User Part (TUP) & ISDN User Part (ISUP)*:
 361 ISUP enables network connections (e.g., call setup, re-
 362 lease). It provides services associated with call set up and
 363 termination[67]. It contains following types of messages:

- 364 • Initial address message (IAM)
- 365 • Subsequent address message (SAM)
- 366 • Address complete message (ACM)
- 367 • Call progress (CPG)
- 368 • Answer message (ANM)
- 369 • Connect (CON)
- 370 • Release (REL)
- 371 • Release complete (RLC)

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

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

- 383 • Integrity of data.

- Authentication of data origin. 384
- Anti-replay protection. 385
- Confidentiality (optional). 386

387 5) *Mobile Application Part (MAP)*: The SS7 protocol was
 388 initially designed to initiate and terminate a voice call. Later
 389 it was modified to include extra features. One of the most
 390 important modifications with respect to scope of this paper was
 391 introduction of MAP which is an application layer protocol. It
 392 was defined by the 3rd Generation Partnership Project (3GPP).
 393 Its basic functionalities include seamless handover, mobility
 394 management, roaming services, short message, and location
 395 services along with many other additional services. It provides
 396 81 different services [73]. The most important entities in the
 397 core network like Mobile Switching Centre (MSC), Home
 398 Location Register (HLR), Visitor Location Register (VLR),
 399 Short Message service centre (SMSC) and Equipment Identity
 400 Register (EIR) use MAP messages to ensure above mentioned
 401 services. The idea behind development of MAP is to allow
 402 communication between different data bases and switching
 403 centres for coordination and location management.

404 3GPP has released an extension of MAP protocol for secu-
 405 rity at application layer[75]. It also mandates use of MAPSec
 406 at network layer in case of IP is being used as a transport
 407 layer.

408 It has three modes

- Protection mode 0-No protection. 409
- Protection Mode 1-Integrity Protection 410
- Protection Mode 2-Confidentiality and Integrity protec- 411
tion 412

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

D. GSM Core Network Elements

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

418 1) *Mobile Switching Centre*: MSC is an interface between
 419 radio and the fixed network of a service provider. Basic
 420 functions of MSC include routing of calls, short messages,
 421 and to ensure seamless handover of calls with other MSCs. If
 422 an MSC has the ability to forward calls and messages to the
 423 MSCs of other networks, it is called gateway MSC (GMSC)
 424 [76].

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

436 3) *Authentication Centre (AuC)*: Its function is to authenti-
 437 cate a user before giving permission to access the network. It
 438 stores the pre shared cryptographic keys and identities of the
 439

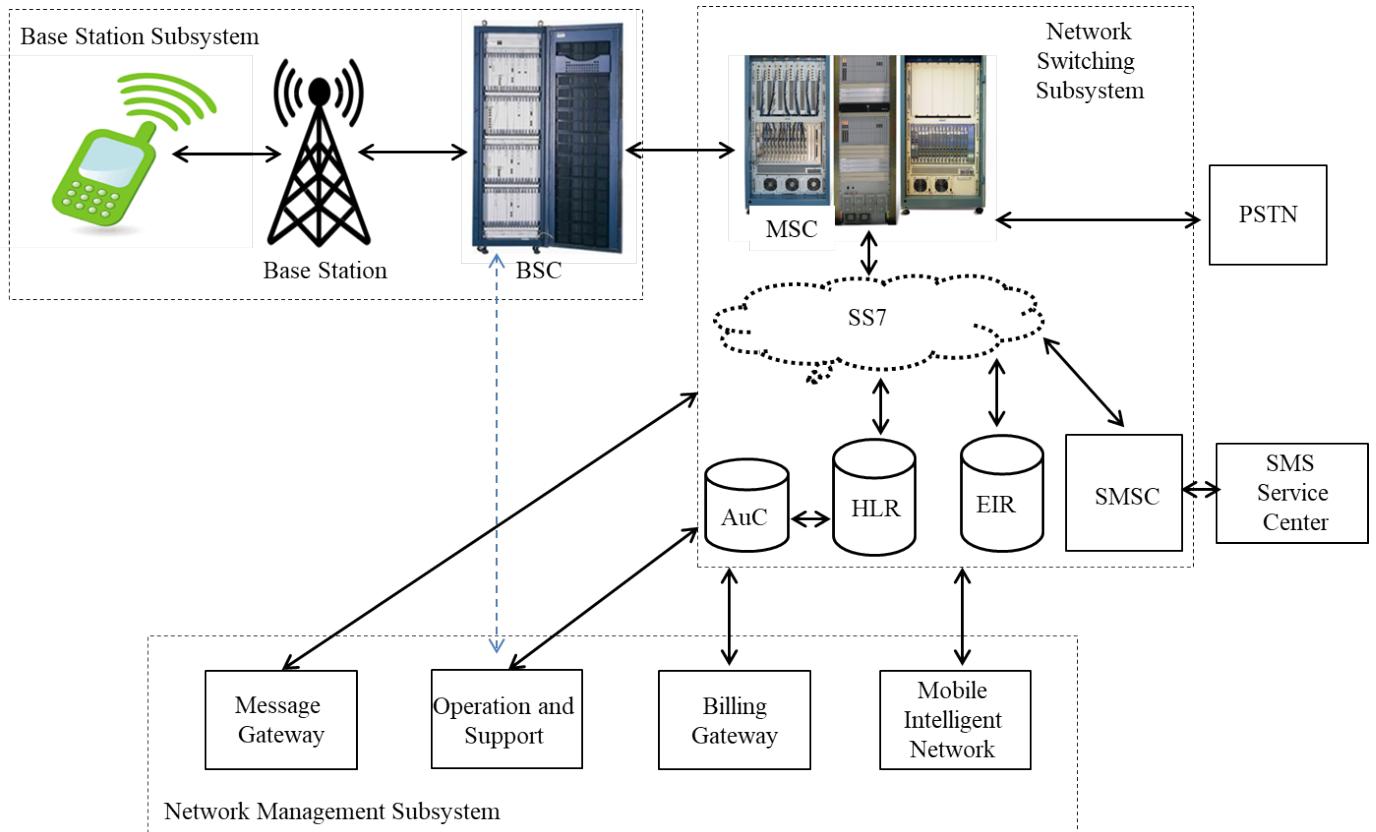


Fig. 6. GSM core network subsystems, elements, databases, and components which are responsible to connect the two users [77].

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

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

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

459 *6) Short message service centre (SMSC):* SMSC is used to
460 route short messages directly to the desired MSC or SMSC.
461 It communicates with HLR to fetch the whereabouts of the
462 user and forwards the message directly to the serving MSC
463 without sending it to HLR or home MSC [79]. It also stores
464 the incoming messages, then forwards them to the destination
465 [80].

466 *7) Identifiers Used in the Core Network:* Various terminolo-
467 gies and identifiers are used as defined by 3GPP in the core

468 network to identify a user and equipment. Each cell phone
469 is uniquely identified by IMEI [81]. International Mobile
470 Subscriber Identification (IMSI) is a 15 digit number which is
471 used to identify a Subscriber Identity Module (SIM). It is the
472 identity of the subscriber and is kept secret. It is used within
473 core network only. It is also used to identify and authenticate
474 a SIM when it access to a network [82]. Mobile Station ISDN
475 (MSISDN) is the number of SIM which is used to call to a
476 particular individual. It is mapped with IMSI and this mapping
477 is maintained in core network[82]. Global Title (GT) is used
478 to identify each element in the network for communication
479 with each other for routing and management of calls [73].

III. GAINING ACCESS TO SS7 NETWORK

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

- 483 • Access to the SS7 network.
- 484 • Ability to map core network entities.
- 485 • Ability to impersonate as any entity within the SS7
486 network.
- 487 • Ability to generate and receive messages to and from core
488 network entities
- 489 • Ability to store, modify and forward messages and calls.

490 From above stated assumptions, the most important and dif-
491 ficult is to get access to the SS7 network. Once attacker has
492 gained access to the SS7 core network, rest of the capabilities
493 depend on professional knowledge and skill set of the attacker

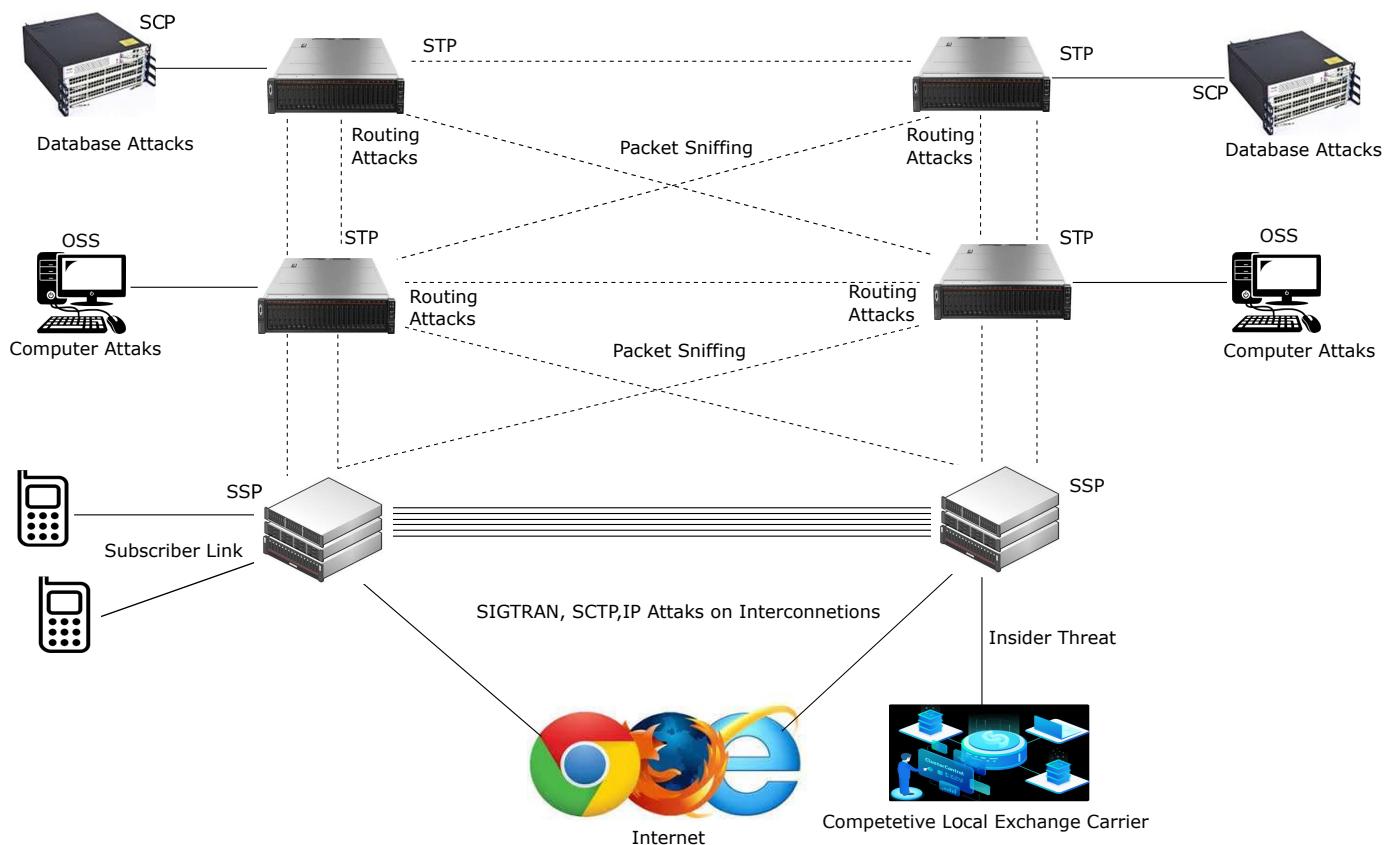


Fig. 7. Attack vectors for entry into the SS7 network [5] - Routing attacks can compromise SCTP, Database attacks against SCP can be materialized, vulnerabilities of SIGTRAN/ SCTP/ IP protocols can be exploited on interconnections of the SS7, and packet sniffing is possible within the SS7 network.

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 sell 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.

546 *C. Misconfiguration of Equipment.*

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

560 *D. Exploiting a Femtocell.*

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

567 *E. Exploiting SIGTRAN Protocol.*

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

585 *F. Exploiting Remote Access of Core Network Entities.*

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

598 *G. Exploiting Operations Support System (OSS).*

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

604 *H. Exploiting Signalling Gateway.*

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

613 *I. Exploiting Local Number Portability (LNP) Feature.*

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

621 *J. KNOWN SS7 ATTACK TYPES*

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

626 **IV. SS7 ATTACKS**

627 *A. LOCATION TRACKING SCENARIOS*

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

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

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

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

653 2) *Exploiting Call Setup Procedure for Location Tracking:*

654 There are no inherent security controls and authentication
 655 mechanism within the SS7 core network. The attacker suc-
 656 cessfully exploits the above mentioned procedure. she can
 657 extract the IMSI associated to the subscriber, GT of MSC,
 658 and roaming number in case a subscriber is roaming in other
 659 network [36]. This attack, as shown in Fig. 9 is accom-
 660 plished in following way:

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

- 672 • HLR will forward this information to the attacker. 672
 Though GT Numbering of MSC is operator specific, but 673 certain fields are mandatory for routing purpose i.e Mobile 674 Country Code (MCC) and Area Code which could narrow the 675 location of a subscriber down to MSC area. It can be a bigger 676 area in urban localities and a smaller area in populated cities. 677 Other options can be exploited to map MSC codes with a 678 geographical area. Known user locations can be queried by 679 the attacker to map the area with MSC GTs [47]. Moreover 680 MSRN can be used to make a call directly to the subscriber 681 with a local number of the visited country. This will avoid legal 682 interception of call by home network and roaming charges. 683

684 3) *Short Message Services(SMS):* SMS sending/ receiv- 684
 ing mechanism is completed in two parts [79][95]. Mobile 685 Originating (MO) Short Message Service transfer and Mobile 686 Terminated (MT) short message service transfer is described 687 as under:

- 688 • Subscriber A types a message and sends it to MSC 688 via BTS which includes text of short message, recipient 689 MSISDN and address of SMSC. 690
 • MSC sends MAP MO Forward Short Message to the 691 specified SMSC. SMSC sends acknowledgement of suc- 692 cessful storage of this message. 693

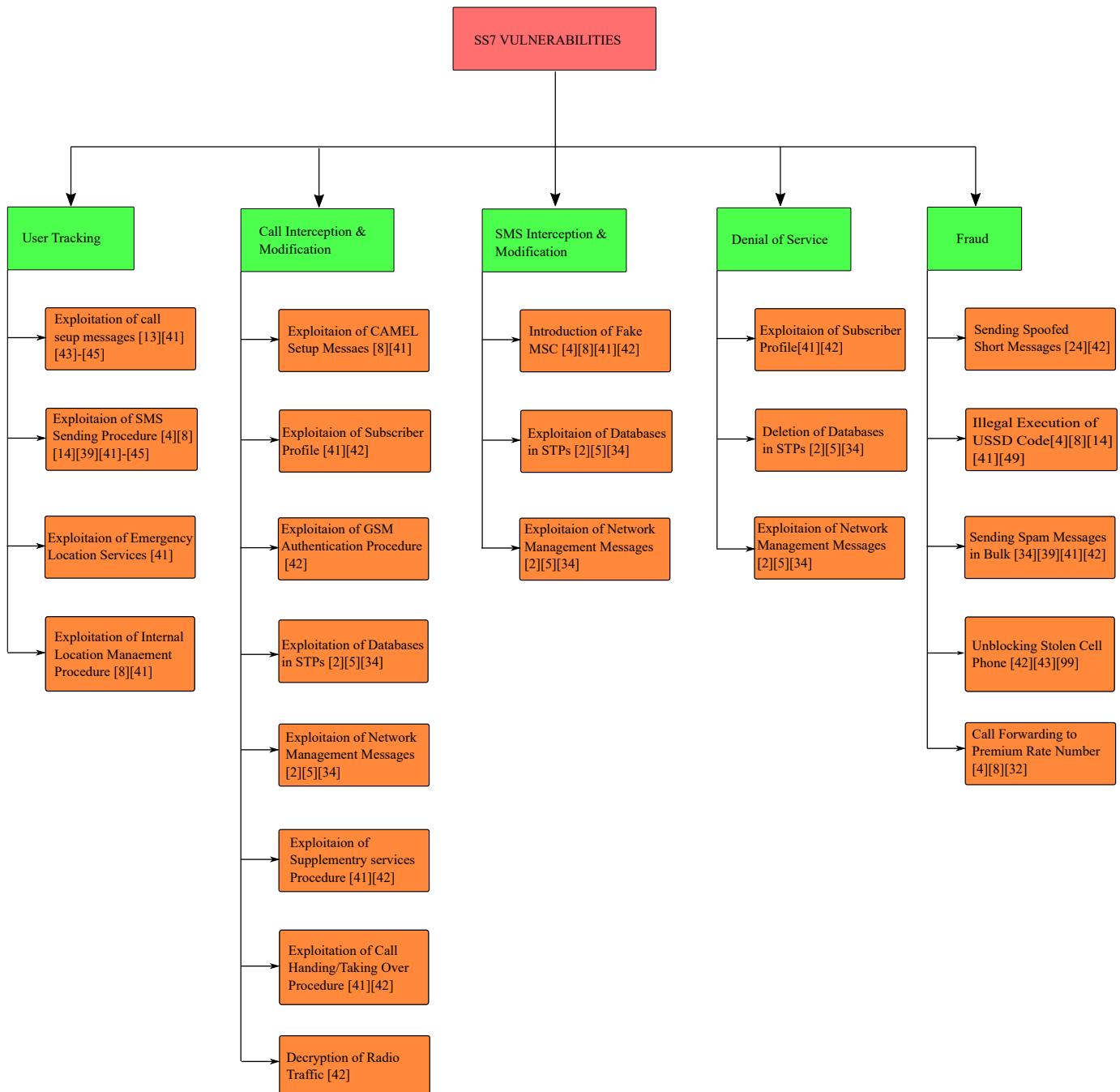


Fig. 8. SS7 attack vectors - This schematic diagram shows list of known methods which can be used to exploit the SS7 network vulnerabilities.

- 695 • SMSC has only MSISDN of the recipient. It needs IMSI
696 of recipient and GT of serving MSC to forward this short
697 message to the destination. This information is stored in
698 HLR of recipient.
- 699 • SMSC sends MAP Send Routing Information for Short
700 Message (MAP SRI SM) request to HLR of recipient
701 which indicates SMSC wants to send a short message to
702 the indicated subscriber and needs its corresponding IMSI
703 and address of serving MSC.
- 704 • HLR replies with MAP SRI SM acknowledgement to
705 SMSC which contains IMSI and GT of serving MSC.
706 SMSC forwards short message to the serving MSC which

- 707 in turn forwards the message to the recipient.
- 708 • If the subscriber is roaming outside the network, then
709 HLR sends MAP PRN request to the MSC in the roaming
710 network which acknowledges with the MSRN. This
711 information along with IMSI and GT of serving MSC
712 is forwarded to the SMSC. SMSC then forwards short
713 message directly to the serving MSC in the roaming
714 network.

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

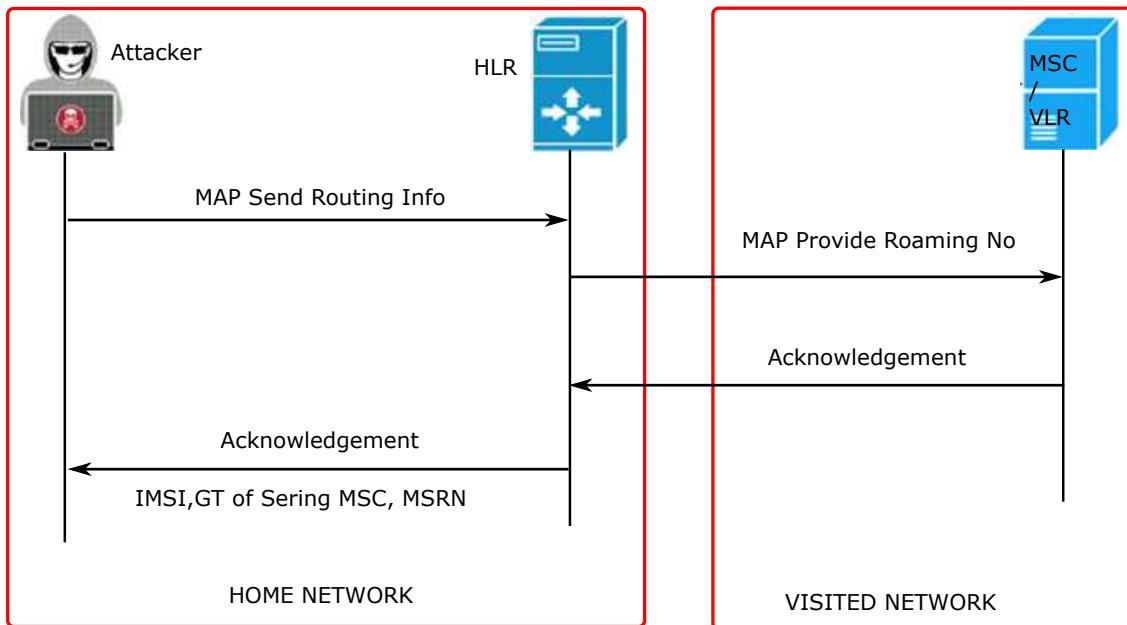


Fig. 9. Location disclosure by exploiting call setup messages [13] - In this method, attacker impersonates as GMSC and asks HLR for whereabouts of victim. HLR replies with IMSI of the user and address of serving MSC where victim is present.

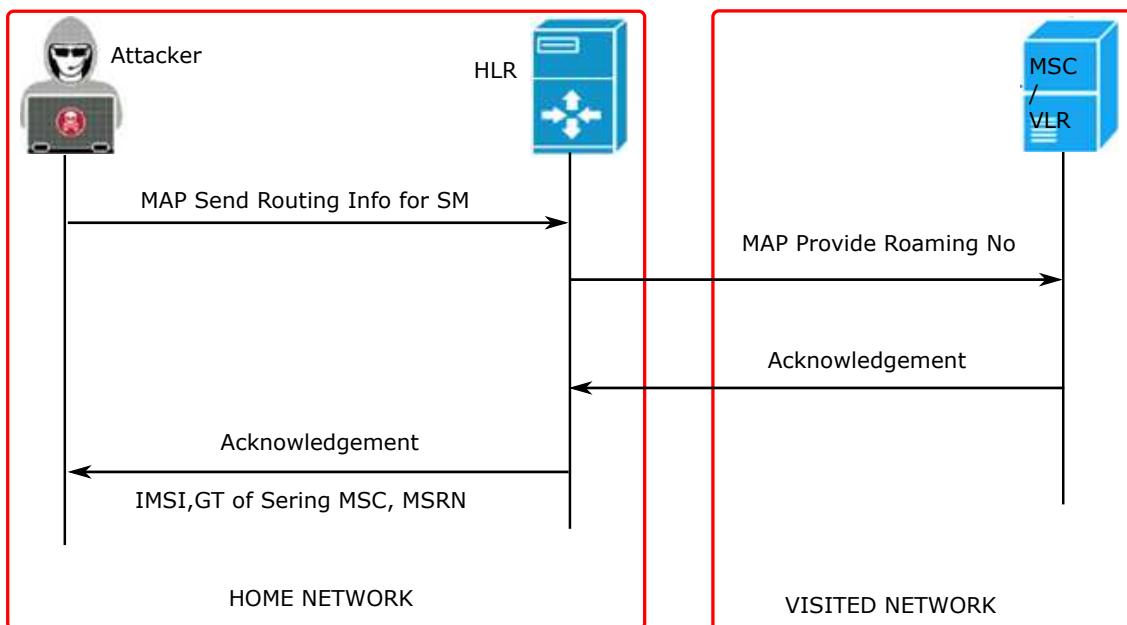


Fig. 10. Location disclosure using SMS procedure [46] - In this case, attacker impersonates as SMSC and asks HLR for address of victim, indicating that it has a short message for victim. HLR replies with IMSI and address of serving MSC.

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

727 5) Internal Location Management Using CAMEL Mes-
728 sages: Service operators can use CAMEL [96] messages to

729 know the location of a subscriber for internal management and
730 to provide location to certain applications which require the
731 position of the subscriber. MAP Any Time Interrogation (MAP
732 ATI) message is used for this purpose. The normal message
733 flow [97] which takes place for the above mentioned service
734 is as under:

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

739 has address of serving MSC but not the exact location.
 740 HLR sends MAP Provide Subscriber Information (MAP
 741 PSI) message to the serving MSC/VLR.

- 742 • MSC sends a paging request to check the latest location of
 743 cell phone. If cell phone is on a call then current location
 744 is forwarded otherwise location at which MSC served it
 745 last time is forwarded.
- 746 • MSC acknowledges MAP PSI message which contains
 747 associated IMSI and cell ID where the subscriber is
 748 located to HLR.
- 749 • HLR sends MAP ATI acknowledgement message to gsm-
 750 SCF which contains the above mentioned information.

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

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

766 *7) Combination of SMS and Internal Location Management*
 767 *Attacks.:* Some network operators have started to block MAP
 768 ATI message due to security and privacy concerns since 2015
 769 [46]. If this message is blocked, HLR will not respond to
 770 MAP ATI message. However the attacker can query location
 771 of a subscriber directly from MSC bypassing HLR. It requires
 772 IMSI and GT of serving MSC which can be obtained through
 773 short message attack (MAP SRI SM). The attack sequence is

774 shown in Fig. 12:

- 775 • Attacker impersonates as SMSC by sending MAP SRI
 776 SM request to HLR for serving MSC address of sub-
 777 scriber .
- 778 • As described earlier, HLR provides associated IMSI and
 779 GT of serving MSC/ VLR without any check/ authenti-
 780 cation.
- 781 • In next step, attacker impersonates as HLR and sends
 782 MAP ATI message to the serving MSC/VLR.
- 783 • MSC sends a paging request to check the latest location
 784 of cell phone considering it as a legitimate request.
- 785 • After receiving the latest location, MSC forwards MAP
 786 ATI acknowledgement message to the attacker which
 787 contains IMSI and cell ID where subscriber was served
 788 last time/ being served

789 *8) Requirement of Emergency Location Service (LCS):*

790 Emergency services need the exact location of the calling
 791 party to provide immediate assistance as per location services
 792 guidelines [98]. The exact location can be found by different
 793 methods like forwarding the GPS location or through triangu-
 794 lation method. This procedure is initiated from the user side to
 795 facilitate the location of the user in distress. Same can be done
 796 from network side as well, which is used to track suspicious
 797 targets by law enforcement agencies. The scope of this paper
 798 is to analyse attacks from network side because the attacker
 799 is within the SS7 network and is acting as one of the entities
 800 of the core network, so we will discuss this scenario only.

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

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

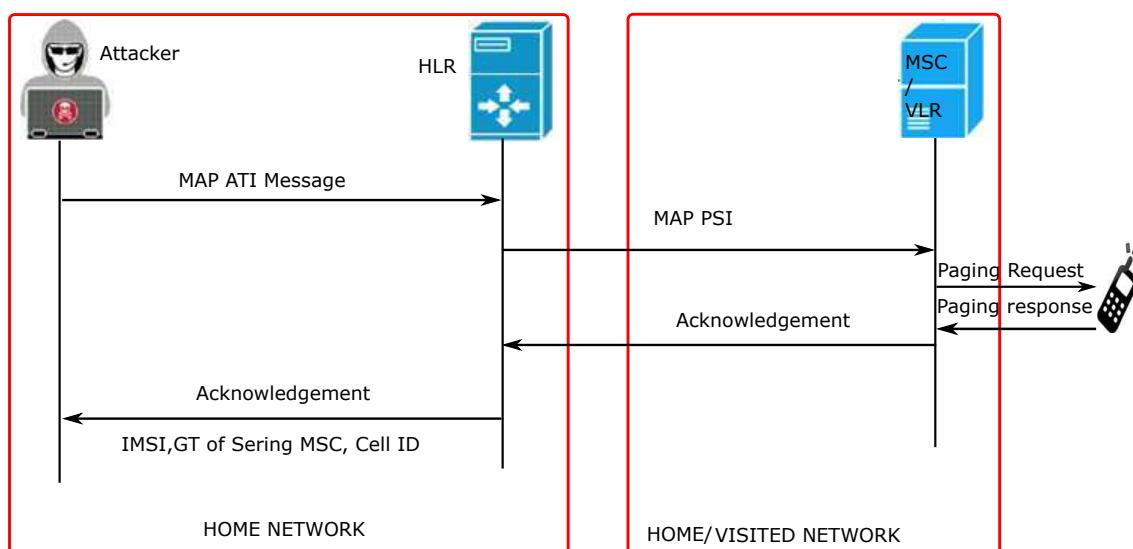


Fig. 11. Location disclosure using ATI message [46] - Attacker gets cell ID and IMSI of the subscriber by sending MAP ATI message, impersonating as gsmSCF. HLR considers it as a legitimate request and sends MAP PSI message to serving MSC/ VLR which determines the location of subscriber through paging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

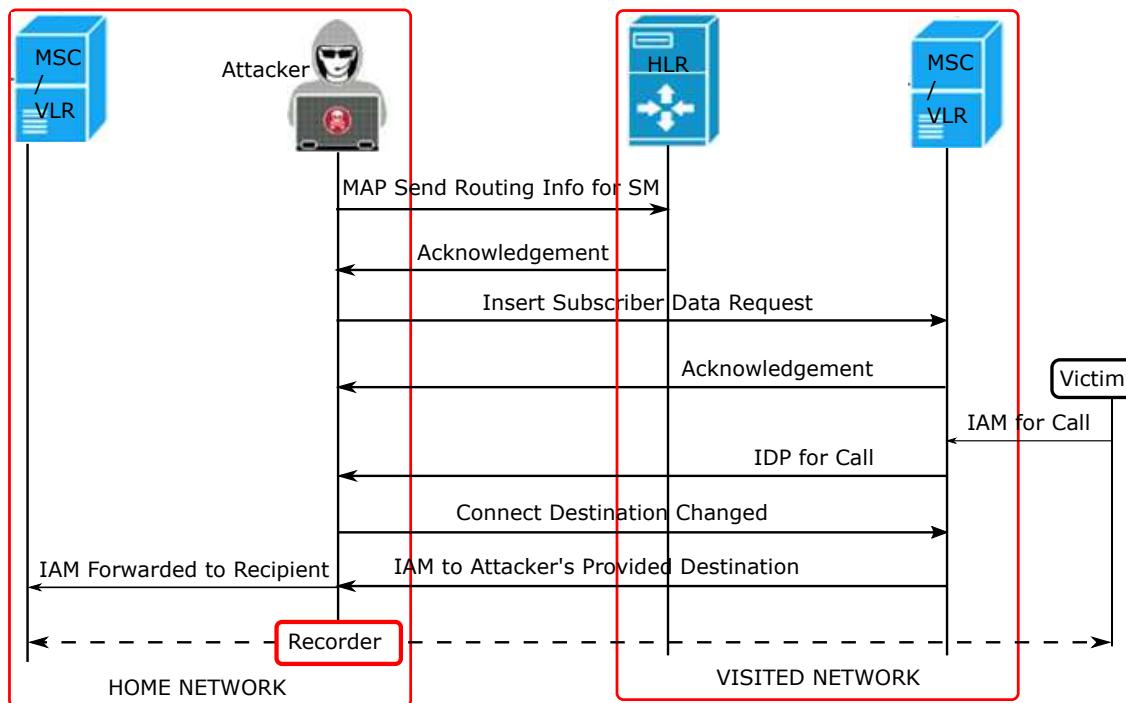


Fig. 12. Location disclosure using hybrid attack [13] - It is combination of SMS and Internal Location Management Attacks. Attacker impersonates as SMSC and gets serving MSC address of subscriber by sending MAP SRI SM request. Then, attacker impersonates as HLR and sends MAP ATI message to the serving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

- 809 • GMLC authenticates the requesting entity. After success-
 810 ful authentication, it sends MAP SRI LBS request to the
 811 HLR.
 812 • HLR replies with MAP SRI LBS acknowledgement to

- 813 GMLC which contains the GT of serving MSC/ VLR in
 814 either own network or visited network in case of roaming
 815 subscriber (it will also contain MSRN).
 816 • GMLC sends Provide Subscriber Location request to the

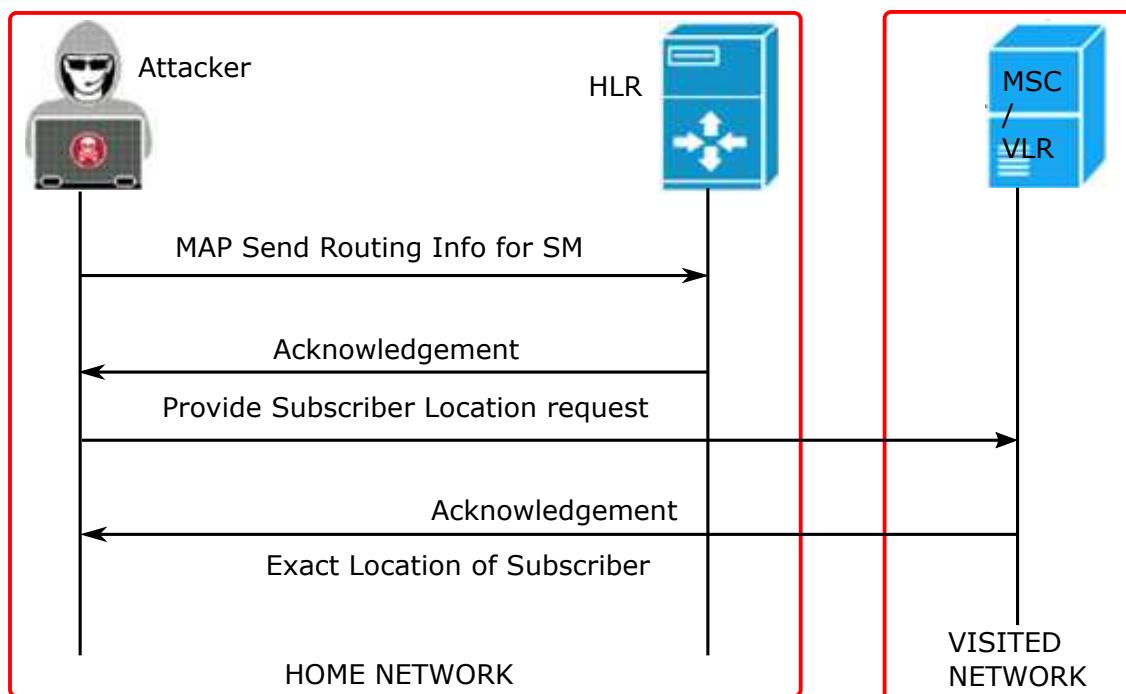


Fig. 13. Location disclosure using LCS message [13] - Attacker gets IMSI and address of serving MSC from HLR. Then, attacker impersonates as GMLC and sends Provide Subscriber Location request to the serving MSC. Serving MSC returns location of victim to the attacker.

817 serving MSC.

- 818 • MSC sends Perform Location Request message to BSC.
819 BSC forwards this request to Serving Mobile Location
820 Centre (SMLC) which performs location request using
821 Radio Resource LCS Protocol [100].
822 • Upon receiving exact location, SMLC answers with Per-
823 form Location Request Response to MSC which forwards
824 this information to GMLC.
825 • GMLC forwards location of subscriber to the client.

826 *10) Exploiting Emergency Location Services for Tracking:*

827 As we have seen in the normal LBS services procedure, ver-
828 ification of requesting entity is done by GMLC. The attacker
829 needs to bypass this verification [10]. Attacker completes this
830 task by adopting following method as shown in Fig. 13:

- 831 • The attacker sends MAP SRI SM containing MSISDN,
832 impersonating as SMSC, to get associated IMSI and
833 address of serving MSC from HLR.
834 • After receiving this information, the attacker imperson-
835 ates as GMLC and sends Provide Subscriber Location
836 request to the serving MSC.
837 • Serving MSC considers it a legitimate request and pro-
838 ceeds as per normal procedure described above and
839 obtains exact location of victim. At the end MSC forwards
840 exact location of subscriber to the attacker.

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

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

853 **B. CALL INTERCEPTION SCENARIOS**

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

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

- 865 • When a user enters in a roaming network, she registers
866 herself with one of the MSCs (Visited MSC) of roaming
867 network with which the home network has roaming
868 agreement.
869 • VMS sends MAP Update Location Request to HLR of
870 subscriber's home network. This message contains GT of
871 VMS along with other parameters.

- 872 • HLR saves the address so that all calls and short messages
873 can be routed through that VMS for the subscriber in
874 future.

- 875 • HLR sends MAP Insert Subscriber Data message to
876 VMS which contains subscriber's profile information,
877 security details and address of its gsmSCF with a list
878 of events to be reported to the home network for the
879 particular subscriber.

- 880 • If the subscriber makes a call to home country without
881 country code, VMS does not recognise the format of
882 dialled number and asks gsmSCF of subscriber's home
883 network about instructions regarding the call. gsmSCF
884 converts the dialled number from local format to interna-
885 tional format by inserting country code and tells VMS
886 to forward the call on the modified number.

- 887 • VMS forwards this call to the MSC of called party.

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

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

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

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

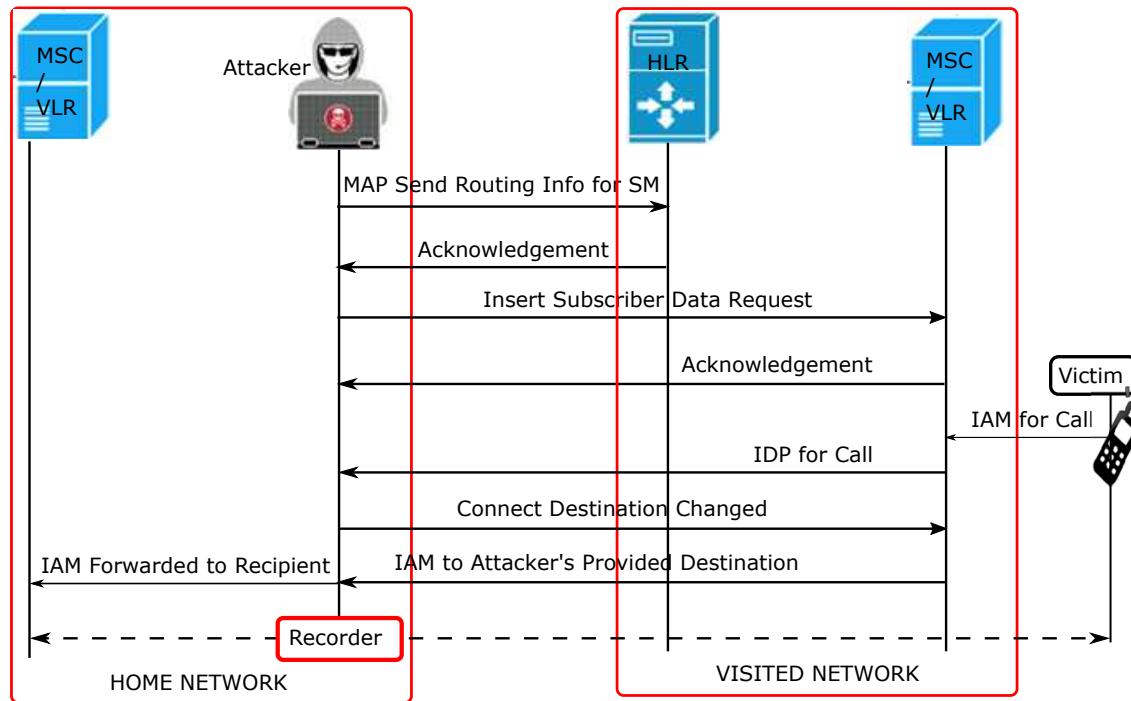


Fig. 14. Call interception by exploiting roaming procedure [47] - Attacker gets address of serving MSC, IMSI and MSRN of subscriber. Then the attacker acts as home HLR and sends MAP Insert Subscriber Data to VMSC which contains a list of events and address of malicious gsmSCF at which those events need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

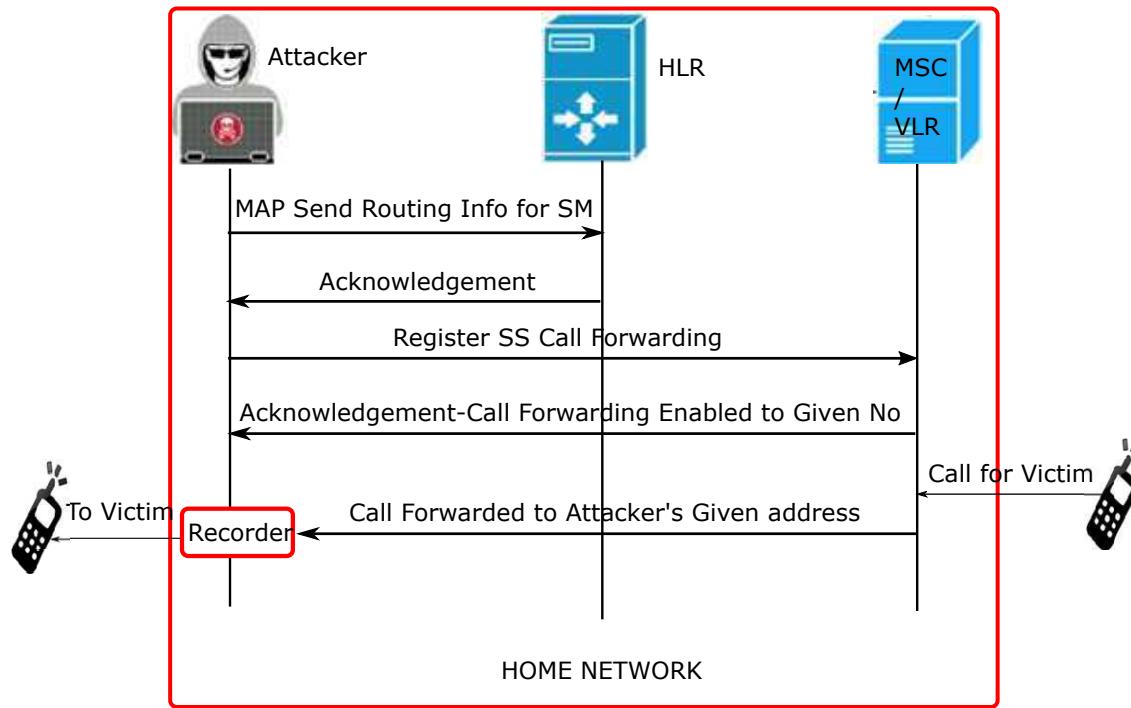


Fig. 15. Exploiting supplementary services[46] - Attacker gets IMSI and address of serving MSC of victim through MAP SRI SM. Then attacker acts as HLR and sends MAP Register SS message to MSC indicating to enable call forwarding to a particular number.MSC enables call forwarding to the desired number.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

- | | |
|---|--|
| <p>929 MSC enables call forwarding to the desired number and
930 acknowledges the message.
931 • Once a call is received for the victim, MSC forwards call
932 to attackers provided number in previous step.</p> | <p>933 • Attacker can record and forward the call to the victim.
934 MAP Erase SS message can also be used by the attacker
935 to disable call forwarding.
936 • Attacker enables the call forwarding to her own premium</p> |
|---|--|

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

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

- 945 • Attacker needs to know the IMSI and GT of the serving
 946 MSC of the subscriber for which she intends to intercept
 947 calls. She gets this information with MAP SRI SM
 948 request from HLR.
- 949 • Attacker acts as MSC and sends MAP Update Location
 950 Information message for the victim subscriber to HLR,
 951 which shows that the subscriber is being served by that
 952 MSC.
- 953 • HLR considers that subscriber has moved to the new
 954 area and is now being served by the MSC which has
 955 sent the message. It sends MAP Insert Subscriber Data
 956 message to the attacker which contains security related,
 957 and subscriber profile information (subscription package,
 958 address of billing platform, and other details).
- 959 • Attacker notes down the contents of this message and
 960 sends another MAP Update Location Information message
 961 to HLR which contains the address of actual serving
 962 MSC which was retrieved in first step.
- 963 • HLR sends MAP Insert Subscriber Data message to MSC.
 964 It is considered a legitimate message as MSC assumes the
 965 user has changed her package subscription.
- 966 • The attacker impersonates as HLR and sends another
 967 MAP Insert Subscriber Data message to MSC with the
 968 same contents as noted in step 4, except for the address
 969 of billing platform which is replaced with a malicious
 970 address. MSC again accepts the changes by taking it as

971 a change in subscription package by the user.

- 972 • When victim makes a call, MSC forwards Initial Detection Point (IDP) message to billing platform for charging
 973 purposes. The address of billing platform is malicious and
 974 is controlled by the attacker. Attacker rewrites the number
 975 with one of her proxies and allows MSC to forward call
 976 to the new number.
- 977 • MSC sends IAM to the destination which is a recording
 978 proxy set up by the attacker. This proxy connects the
 979 calling party with destination and records all calls in
 980 the middle. As the call is finally being forwarded to its
 981 destination, so the victim never knows that her call is
 982 being recorded or intercepted.

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

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

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

- 1000 • The attacker intercepts call on air interface using some
 1001 custom made device for this purpose. The Attacker needs
 1002 to be in the vicinity of the victim. As call is encrypted,
 1003 the attacker needs the decryption keys to decrypt it.

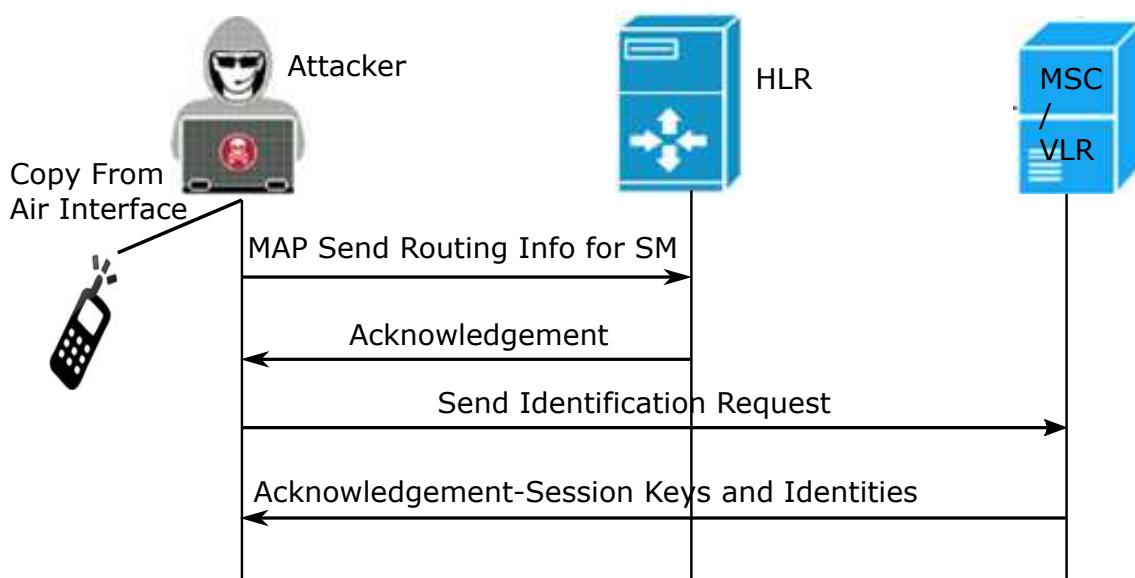


Fig. 16. Intercepting calls by decrypting radio traffic [47] - Attacker intercepts encrypted call on air interface. Attacker impersonates as MSC and gets session keys needed to maintain the call by sending MAP Send Identification message to serving MSC for taking over the call. serving MSC shares session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

- 1005 • Using MSISDN of the victim, attacker retrieves IMSI and
1006 GT of serving MSC from HLR through MAP SRI SM
1007 attack impersonating as SMSC.
- 1008 • The attacker impersonates as MSC and sends MAP Send
1009 Identification message to serving MSC. Serving MSC
1010 considers that the subscriber is moving and entering into
1011 a new MSC area.
- 1012 • Serving MSC initiates the call handing over procedure
1013 and acknowledges with the session keys needed to main-
1014 tain the call.
- 1015 • The attacker receives the keys and is already copying
1016 call on air interface, the handover never takes place and
1017 attacker can decrypt the call in a live attack or can save the
1018 call to decrypt it later [44]. Temporary Mobile Sub-
1019 scriber Identity (TMSI) can provide some defense in identifying
1020 the particular user over air interface. It is assumed that
1021 the attacker has gained TMSI through some other method
1022 which is out of scope of this paper.

1023 C. SMS INTERCEPTION AND FRAUD CASES

1024 There are numerous SMS fraud cases, however, in this
1025 section only those cases are discussed which exploit loopholes
1026 in the SS7 network.

1027 1) *SMS Interception Using Fake MSC*: A Short Message
1028 Service (SMS) is delivered in two parts in following way:

- 1029 • Sender sends the short message to the SMSC through
1030 MSC which is called Mobile Originated (MO) part.
- 1031 • SMSC forwards this short message to serving MSC which
1032 subsequently delivers it to the recipient and is called
1033 Mobile Terminated (MT) part.
- 1034 • It is prudent to mention here that mobile originated
1035 forward short message received by SMSC has no authen-
1036 tication mechanism and therefore can be exploited by the
1037 attacker for malicious purposes.
- 1038 • In this attack, the aim of the attacker is to receive, store,
1039 modify all short messages of a particular subscriber, and

1040 then forward these messages to the recipient. Message
1041 flow of attack is shown in Fig. 17. The attacker imperson-
1042 ates as SMSC and sends MAP SRI SM for a subscriber
1043 to HLR by enclosing MSISDN of the subscriber.

- HLR acknowledges with MAP SRI SM reply which
1044 contains the IMSI and GT of the serving MSC.
- The attacker has learned IMSI and GT of serving MSC.
1045 Now the attacker acts as VMSC and sends MAP Update
1046 Location message for that subscriber using received IMSI
1047 to home HLR. This message shows that subscriber is
1048 being served by that VMSC. HLR saves the address of
1049 the VMSC for future.
- When another subscriber sends a short message to the
1050 victim, SMSC of sender contacts HLR of the victim
1051 through MAP SRI SM request.
- HLR has the address of victim which was provided by the
1052 attacker as serving MSC. It forwards the same to SMSC
1053 in acknowledgement message as the GT of serving MSC
1054 for the victim.
- Sender's SMSC forwards short message to the fake MSC
1055 which is received by the attacker who can copy, modify,
1056 and then forward it to the actual recipient.
- The victim number is continued to be compromised until
1057 she enters into a new MSC area and her location is
1058 updated to the HLR. Until then the attacker intercepts
1059 all short messages of the victim including one time
1060 passwords for financial transactions, authentication codes
1061 from social networks, and other important messages.

1062 2) *Exploiting Mobile Originated Forward SM Part*: As
1063 there is no authentication check on mobile originated forward
1064 short messages and mobile terminated forward short message
1065 parts, they can be exploited by an attacker having access to the
1066 SS7 network. This attack can be used for a variety of purposes
1067 like sending spam messages for commercial purposes and fake
1068 messages or flooding (short messages) attack on a particular
1069 subscriber. This attack can be described as under as shown in

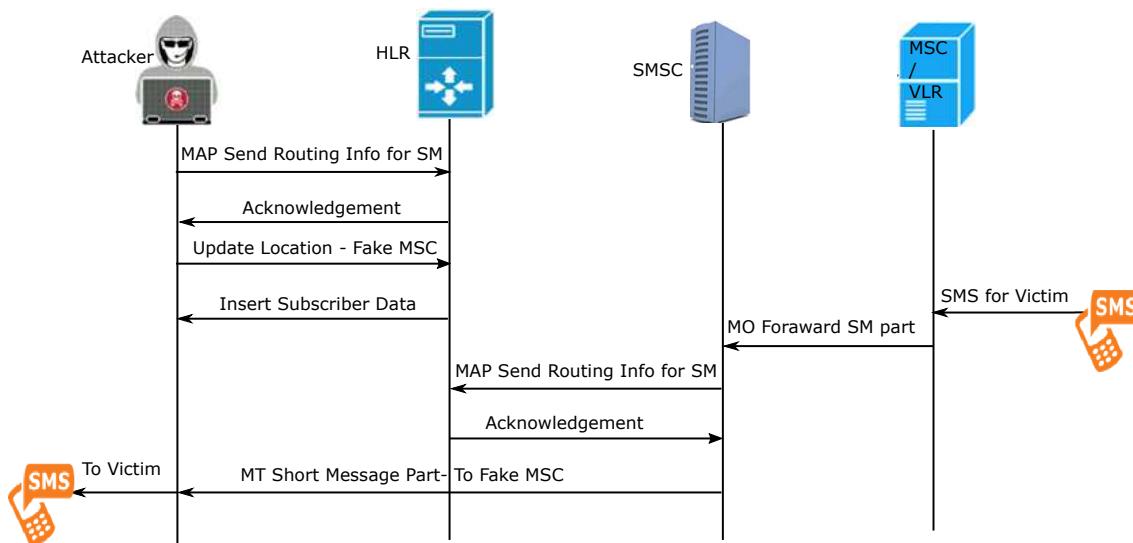


Fig. 17. SMS interception using fake MSC [47] - Attacker impersonates as SMSC, gets IMSI and address of serving MSC of victim. Then attacker acts as VMSC and replaces address of victim with fake MSC in HLR. All short messages will be forwarded to the fake MSC controlled by attacker.

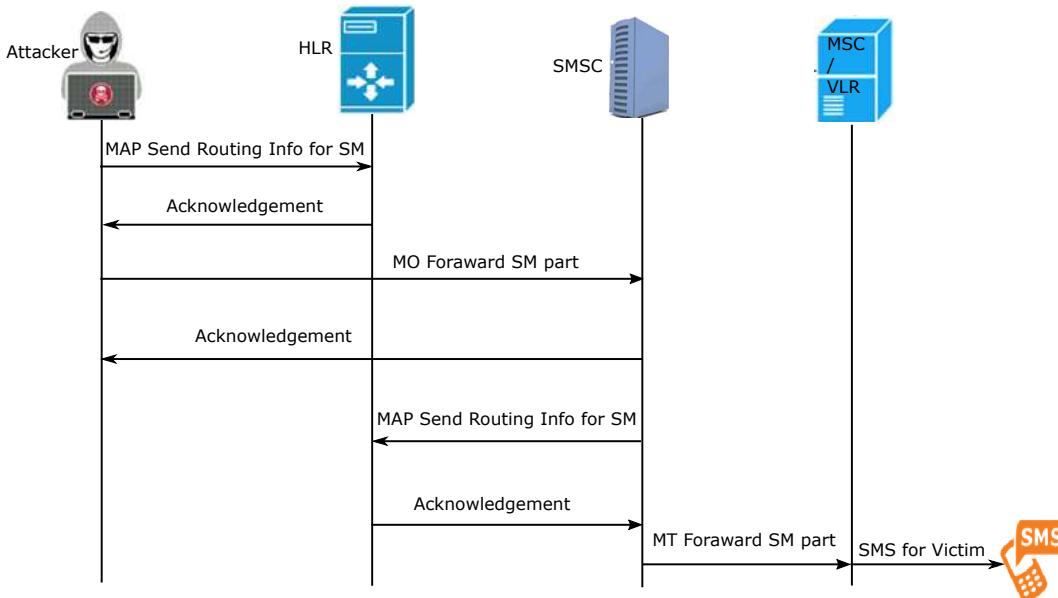


Fig. 18. Exploiting MO forward short message part [47] -Attacker gets IMSI and address of serving MSC for victim through MAP SRI SM. Then, attacker acts as serving MSC for the user on whom behalf she is sending the short message, and forward mobile originated short message part to SMSC. This message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

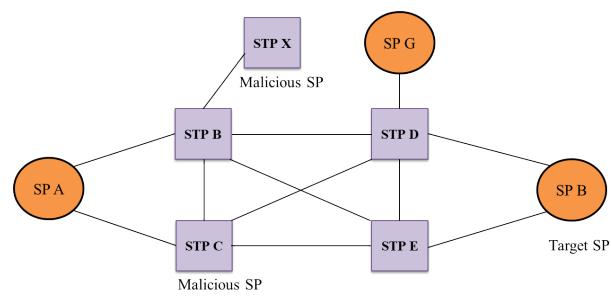


Fig. 19. Exploitation of network management messages [2] - Attacker sends a malicious Changeover Order message to STP B impersonating as SP A. STP B assumes the message is legitimate and stops sending signalling messages to the link reported unavailable in Changeover Order message by the attacker.

1128 4) *Transferring Funds Using USSD*: Some service
1129 providers are giving option of sharing credit through Unstruc-
1130 tured Supplementary Service Data (USSD). USSD code is
1131 executed by the subscriber to send or share the credit [46]. An
1132 attacker having access to the SS7 impersonates as a subscriber
1133 and sends MAP Process USSD message which is executed
1134 without any authentication.

1135 D. DENIAL OF SERVICE (DOS) ATTACKS

1136 DoS attack aims to disrupt the services for a particular
1137 subscriber. When a subscriber moves to a new area and gets
1138 registered with a new MSC, it sends MAP Update Location
1139 message to HLR. After receiving this message, HLR sends
1140 MAP Insert Subscriber Data message to MSC/ VLR [76]. This
1141 message and MAP Delete Subscriber Data message is also sent
1142 to MSC/ VLR when a subscriber changes her subscription
1143 package. These messages contain the details of all activities,
1144 a subscriber is allowed/ not allowed to do. Attacker can use
1145 these messages to deny the subscriber from making/ receiving
1146 calls and sending/ receiving messages [46] in following way:

- 1147 • Attacker collects IMSI and GT of serving MSC through
1148 short message attack (MAP SRI SM).
- 1149 • Attacker acts as HLR and sends MAP Insert Subscriber
1150 Data/ Delete Subscriber Data message to MSC.
- 1151 • This message contain the instructions that subscriber is
1152 not allowed to make/ receive calls and send/ receive short
1153 messages.

1154 E. EXPLOITING NETWORK MANAGEMENT MESSAGES

1155 At MTP 3 layer, network management messages are ex-
1156 changed between two directly connected STPs via C-link to
1157 determine/ convey the status of a route or an SP with respect to
1158 congestion/ non-availability. These messages have no inherent
1159 authentication and integrity check and can be exploited by
1160 the attacker. There are various network management messages
1161 used at this layer but two of them are be discussed in this
1162 section.

1163 1) *Changeover Procedure*: When a signalling link fails or
1164 becomes unavailable for signalling traffic, Changeover proce-
1165 dure is used to re-direct signalling messages from alternate
1166 routes which are available to that destination. The failure is
1167 detected due to high signal error rate, prolonged delay in ac-
1168 knowledgement of sent messages, congestion, and unavailabil-
1169 ity of terminal equipment [104]. When this scenario is detected
1170 by an SP and needs to carry out a Changeover Procedure, it
1171 sends a Changeover Order message to the connected SPs. No
1172 inherent authentication, encryption or integrity mechanism is
1173 involved. The receiving SP checks only the routing label of
1174 the sender (originator address). If routing label is one of the
1175 directly connected SPs, the message is considered legitimate
1176 otherwise it is discarded.

1177 *Exploitation of Changeover Procedure*: We consider the
1178 scenario presented in Fig. 19. Let us suppose STP X is under
1179 control of the attacker and can send malicious management
1180 messages to other nodes [2]. It sends a Changeover Order
1181 message to STP B impersonating as SP A (uses routing label of
1182 SP A). STP B has the only way of checking the legitimacy of

1183 the message is by checking routing label. STP B assumes the
1184 message is legitimate and stops sending signalling messages to
1185 the link reported unavailable in Changeover Order message by
1186 the attacker. If the attacker has capability of sending multiple
1187 messages to STP B with coordination from other nodes, she
1188 can make some signalling links unavailable. Traffic will be
1189 diverted to alternate routes consuming more resources and
1190 decreasing efficiency.

1191 2) *Transfer Prohibited Procedure*: When a particular desti-
1192 nation is unreachable to an STP, it initiates Transfer Prohibited
1193 Procedure (TFP). In this procedure, it informs to adjacent
1194 SPs about the unavailability of a particular destination and to
1195 stop forwarding messages for that destination. A TFP message
1196 contains following information [104]:

- 1197 • Routing label of the originating STP.
- 1198 • Transfer prohibited signal.
- 1199 • Destination address for which messages are not to be
1200 forwarded due to its unavailability.

1201 We consider the scenario given in Fig. 19. STP D has two
1202 routes to transfer messages to SP B. It can deliver messages
1203 directly to B or via STP E. If both the routes become
1204 unavailable, STP D can no longer send messages to SP B.
1205 STP D initiates TFP message to adjacent SPs notifying them
1206 SP B is not available and its messages are not to be routed
1207 through it. All the messages at STP D destined for SP B are
1208 dropped. If there is no alternate route available to other STPs,
1209 they also drop messages destined to SP B.

1210 This procedure can be exploited by an attacker. We consider
1211 SP B is target SP of the attacker. Initially all links are working
1212 and two routes are available for messages destined to SP B. let
1213 us say attacker controls the STP X and sends a malicious TFP
1214 message to STP B impersonating as STP D. It contains the
1215 address of SP B as unavailable destination. Now all the mes-
1216 sages of SP B will be routed through STP E. It has provided
1217 the chance to attacker for traffic diversion. If the attacker has
1218 ability to generate multiple messages or coordinated messages,
1219 she can send TFP messages impersonating as STP E which
1220 also declares SP B unavailable. Then all the messages from
1221 STP B which are destined to SP B will be dropped; creating
1222 a denial of service for SP B.

1223 F. COMPUTER ATTACKS ON CORE NETWORK 1224 ELEMENTS[28].

1225 The attacker can gain full control of the databases/ core
1226 network elements by attacking Operation Support System
1227 (OSS) or remote access application. This situation could be
1228 devastating in many ways as follows:

- 1229 • Re-routing of calls by exploiting and changing various
1230 data bases and customer's record in the SS7 network such
1231 as changing call forwarding and speed dialling numbers
1232 of a particular subscriber or random changes in the data
1233 base to create a chaos.
- 1234 • Exploiting routing tables and GT translation tables gives
1235 opportunity to record calls by forwarding them to the
1236 desired location/routes.
- 1237 • Interception of secret user identities by deploying the SS7
1238 packet sniffers due to no encryption in the core network.

- 1239 • Deletion of routing tables, GT translation tables, call
1240 forwarding data and speed dialling information stored at
1241 various databases can cause interruptions.

1242 These attacks can cause havoc at national level especially
1243 in those countries where only few telecom operators provide
1244 services in the country and each company provides services to
1245 a large portion of population as compromise of one company
1246 will effect a major part of population. Just take the case of
1247 altering call forwarding data base. An attacker alters the call
1248 forwarding data base and sets all call forwarding to emergency
1249 services at the time of a major crises like a terrorist attack or a
1250 natural disaster. It can create a panic because all normal calls
1251 will be forwarded to emergency service centre. This will create
1252 a chaos in the public and can cause delay in rescue efforts.
1253 If GT data base is altered, then the calls will be forwarded
1254 to wrong MSCs/ VLRs where the recipient is actually not
1255 available hence creating a DoS attack.

V. DEFENSES

1256 Defenses against exploitation of the SS7 network have
1257 been proposed by various researchers/ security experts. These
1258 defenses have been summarised in table IV. In this section
1259 defenses of the SS7 are discussed briefly.

A. Critical Security Controls

1260 Following Critical security controls can help in protecting
1261 the SS7 core network [8]:

1262 1) A clear boundary of the network is to be defined. All
1263 messages entering and leaving the network needs to be filtered
1264 and checked whether they have some external usage or not.
1265 The SS7 firewalls and IDS/IPS can be used for this purpose.

1266 2) All the events/ activities and communication in the core
1267 network are to be logged for analysis and audit of network.
1268 Logs are to be maintained through inherent capabilities of
1269 the core network entities or through logging devices deployed
1270 within the core network. Logs are to be analysed and audited
1271 regularly and results are to be evaluated.

1272 3) Network is to be properly segregated. Trust and exposure
1273 level of each element is to be defined and then to be placed
1274 in the network accordingly. Different security zones are to be
1275 established and the network elements need to communicate
1276 with other networks are to be kept in separate security zone.

1277 4) Penetration testing is to be carried out at regular intervals
1278 and after addition/ deletion of devices. This helps in finding
1279 the vulnerabilities and security gaps of the system. Red team
1280 exercises are to be conducted regularly to check system
1281 defenses and to improve response time of the team to counter
1282 any attack.

1283 5) Attacks on the SS7 network are very likely to occur. It
1284 is necessary to maintain and train a team of security experts
1285 to respond the incidents in case of an attack materializes.

1286 6) Best practices should be adopted while configuring core
1287 network elements. They should be hardened, unused services
1288 and accounts are to be blocked, no extra port is to remain open,
1289 and all the settings and management related activities are to
1290 be done from local control on the core network or through a
1291 secure channel.

B. Scrutiny of Signalling Messages

1290 1) MAP insert Subscriber Data message is sent by the home
1291 network of the subscriber to the visited network. This message
1292 is to be authenticated before saving it for future use. Source
1293 network of the message must be checked. Any message which
1294 has been originated other than the subscriber's home network
1295 is to be dropped [47].

1296 2) All requests arriving at HLR are to be processed and val-
1297 idated prior giving any information which contains subscriber
1298 data such as IMSI and whereabouts.

1299 3) Application layer firewalls are to be deployed to filter
1300 out and check MAP and CAP messages leaving or entering
1301 the network. Effective policies and monitoring is to be done
1302 to get desired results.

1303 4) On the subscriber side, there is very less avenue which
1304 can be explored for defense against these attacks. However,
1305 there are some applications like "SnoopSnitch" [105] and
1306 "Darshak" [106] available to be installed on cell phones which
1307 can help in analysis of the subscriber's SS7 traffic and can give
1308 warning of unusual activities.

1309 5) MAP ATI messages are used internally for location
1310 management and need to be blocked due to privacy concerns.
1311 Though some of the service operators in Europe have blocked
1312 these messages but most of the operators in the world are still
1313 using these messages which can be exploited [46].

1314 6) MAP SRI SM message come from other network and
1315 have a legitimate purpose. These messages could be secured
1316 from being exploited with the introduction of SMS home
1317 routing [107]. Without SMS home routing, these messages
1318 are difficult to be identified for their malicious intent.

C. SMS Home Routing

1324 It has been established from attacks explained above that the
1325 attacker necessarily needs the IMSI and GT of serving MSC
1326 to proceed further with her attacks. Both of these identifiers
1327 can be obtained by different methods from HLR. One of the
1328 easiest methods used by the attacker is with the help of MAP
1329 SRI SM. In this scenario the short message is not forwarded
1330 to home HLR of the recipient rather SMSC of the sender
1331 network asks only about the IMSI and GT of serving MSC of
1332 the recipient which is handed over without any authentication.
1333 This method is exploited by the attacker and raises serious
1334 security and privacy concerns. Realizing these threats 3GPP
1335 presented a proposed solution for this problem with the name
1336 of home routing published in 2007 [107][114]. SMS sending
1337 procedure without home routing is shown in Fig. 20 and SMS
1338 sending procedure with home routing is shown Fig. 21. This
1339 modification defined a new way of sending short messages.
1340 Instead of handing over IMSI and serving MSC GT to the
1341 sender, it enabled home network to receive and then forward
1342 the short message to the recipient. This modification requires
1343 a new entity to be installed by each network provider called
1344 SMS-Router. After installation of this router, when an SMSC
1345 will send MAP SRI SM to HLR, HLR will not reply rather
1346 it will forward this message to SMS router. SMS router will
1347 reply with MAP SRI SM Acknowledgement which will be
1348 forwarded to sender's SMSC.

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: <ul style="list-style-type: none"> • Protection mode 0: no protection. • Protection mode 1: Provision of integrity and authentication. • Protection mode 2: Provision of integrity, authentication, confidentiality.
Lingling, Jiang and Ma Hong [39]	2009	It suggests 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: <ul style="list-style-type: none"> • 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

1350 Two major differences in the contents of acknowledgement
1351 messages with SMS router are:

- 1352 • IMSI of the subscriber is not sent rather a mapped value
1353 from SMS router is sent which is only available with
1354 the SMS router. This prevents disclosure of IMSI to the
1355 malicious entities/ attacker.
- 1356 • GT of serving MSC is not forwarded rather GT of
1357 SMS router is sent to sender's SMSC and asked to
1358 forward short message to this address. This makes the
1359 home network overall incharge of short message sending
1360 procedure rather than giving control to sender's SMSC.

1361 This method prevents most of the SMS based attacks described
1362 earlier like spoofed and spam messages. It also provides the
1363 capability of lawful interception of the short messages to the
1364 home network if the subscriber is roaming in another network.
1365 Previously home network was unaware of the contents of short
1366 message if the subscriber was roaming.

D. Use Of MTPSec at MTP3 Layer

1367 Network management messages are exploited due to ab-
1368 sence of any security mechanism between adjacent SPs in the
1369

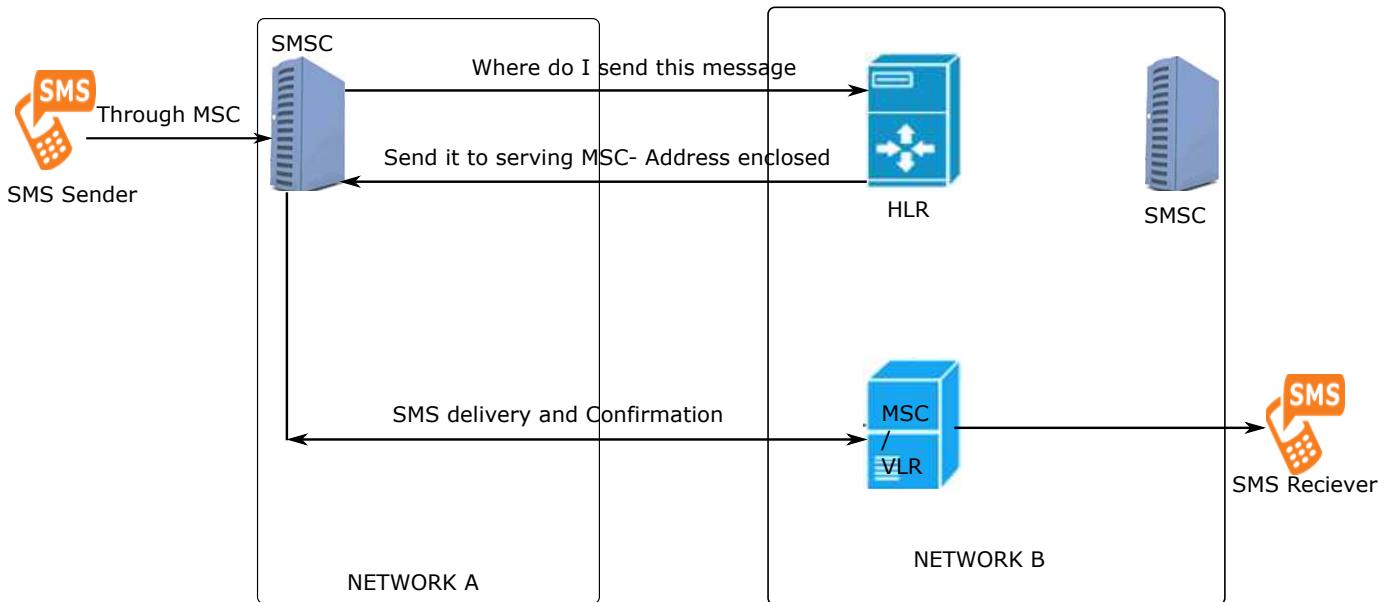


Fig. 20. SMS procedure without home routing [114] - SMSC asks HLR for address of a user to send a message. HLR sends IMSI of the user and address of serving MSC where user is present.

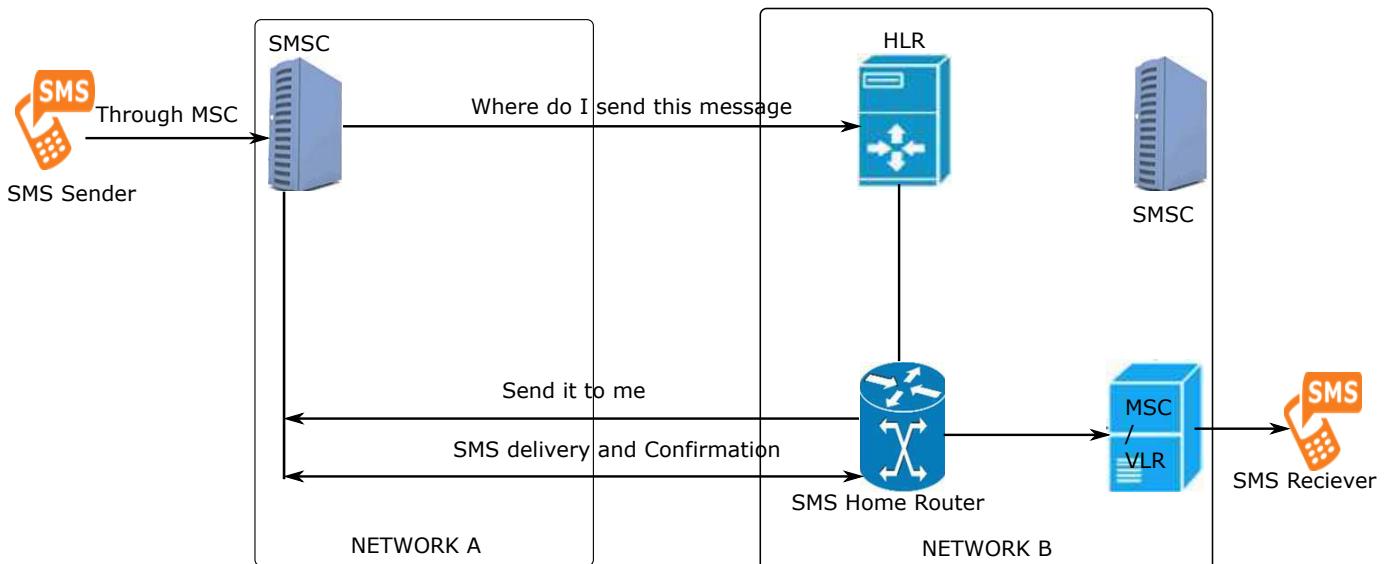


Fig. 21. SMS procedure with home routing scenario [114] - SMSC asks HLR for address of a user to send a message. Address of home router is sent to SMSC. SMSC will send message to home router, home router will forward message to destination. Credentials of the user will not be provided to other network.

1370 SS7 network. To achieve mutual authentication and to enforce
 1371 integrity, a solution was proposed to be used at MTP3 layer
 1372 with the name of MTPSec [2]. This solution consists of two
 1373 protocols namely Key Exchange and Authentication Header
 1374 protocol. These protocols can be used to provide mutual
 1375 authentication between SPs, integrity of the contents of the
 1376 management messages, key generation, and key management.

1377 E. A Conceptual Defense Model

1378 For the prevention and mitigation of attacks, a conceptual
 1379 model is proposed as shown in Fig. 22, based on the SS7
 1380 management system presented in [5] and [47]. This model

is in addition to the deployment of SMS home routing by the
 1381 network provider. The details and specification of the proposed
 1382 components are left to the network provider to choose from
 1383 available options in the market or to develop proprietary
 1384 solutions specific to their needs.

1385 1) *Access Control/ Authentication:* SSPs are the compo-
 1386 nents of SS7 core network which interact with the subscriber's
 1387 device. They are the entry points of an attacker as well. There
 1388 needs to be an access control mechanism to enter into the
 1389 SS7 network. An authentication module on SSPs will serve
 1390 the purpose. It should issue an authentication token or key to
 1391 every legitimate user for access to the network and block all
 1392 other accesses to the network.

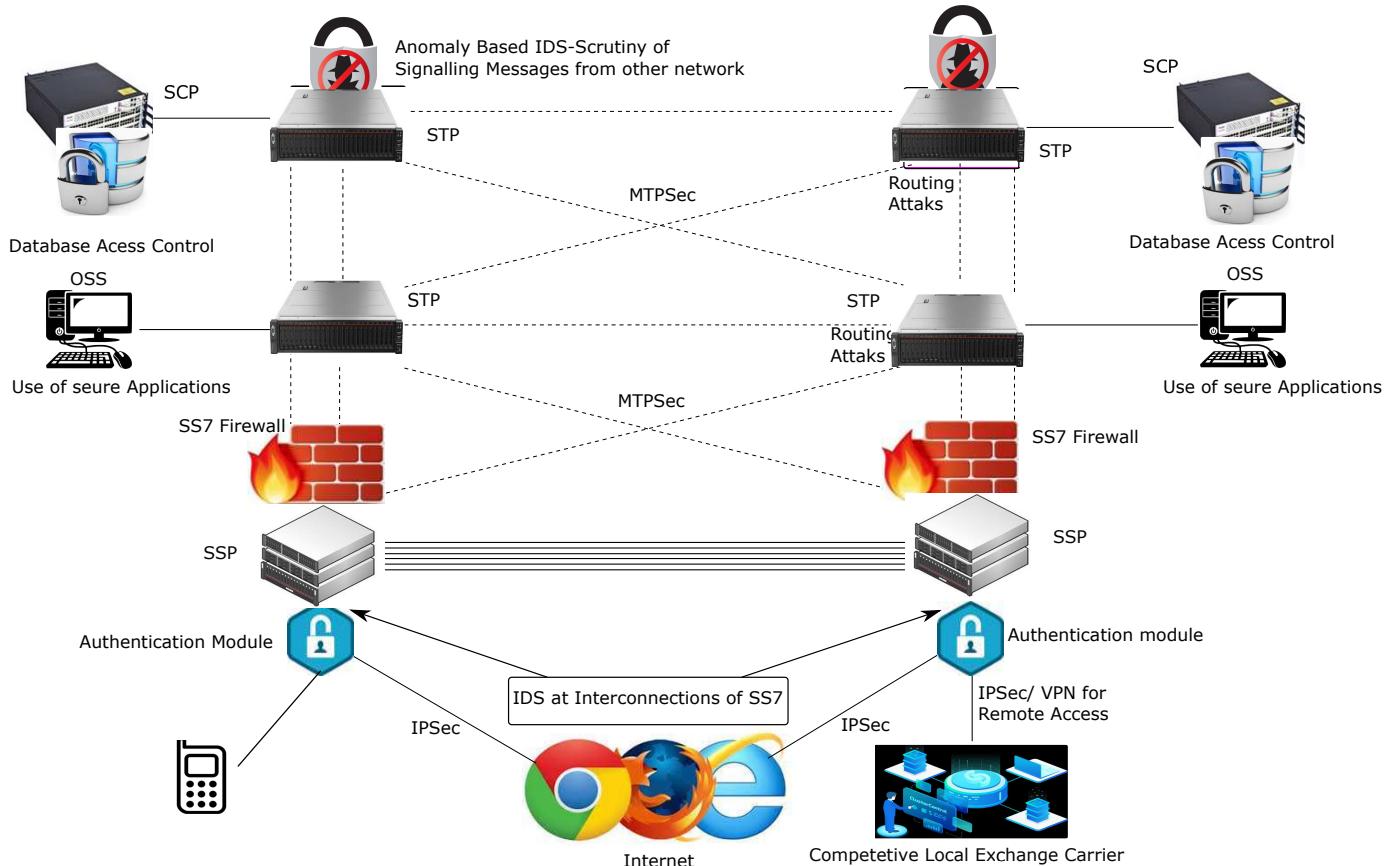


Fig. 22. A conceptual defense model based on [5] - For defense of the SS7 network, access control should be implemented on SCP. Anomaly based detection techniques should be used on STP. MTPSec should be used to avoid sniffing of the SS7 messages. Authentication mechanism should be implemented on SSP.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

1394 2) *Encrypted Authentication:* For cell phone users, au-
 1395 thentication will take place over air interface so it needs
 1396 to be encrypted with session keys, once the user has been
 1397 identified by the network. Every time a user requests for a
 1398 service through SS7 messages, network should authenticate
 1399 the user with the help of authentication token or key, issued
 1400 in previous step. This will prevent attacker from exploiting the
 1401 SS7 network. Messages used for signalling between different
 1402 components of the SS7 network need to be authenticated.
 1403 There should be a mechanism to authenticate the contents and
 1404 origin of the these messages. Cryptographic protocols can be
 1405 used for this purpose. There is no reason that core network
 1406 elements cannot support cryptographic applications. The only
 1407 issue could be the delay in signalling before connecting a call
 1408 and sending a short message. Elliptic curve cryptography [115]
 1409 can be used within the core network which is an efficient
 1410 and lighter encryption system. However for inter-networks
 1411 communication, concept of PKI [116] can be implemented.

1412 3) *Encryption of Signalling Messages:* Signalling messages
 1413 used within the network need to be encrypted so that they
 1414 are not understood by the attackers if they are intercepted.
 1415 Attacker needs to map the core network entities for the
 1416 attack purpose. Encrypted messages will prevent attacker from
 1417 learning about infrastructure of the core network. Virtual
 1418 private network (VPN) [117] can be used between intercon-
 1419 necting operators so that interception of these messages can

be avoided[47]. Another solution is the use of public key
 1420 infrastructure (PKI) Certification Authority (CA) [118] for
 1421 inter-network communication to avoid spoofing and to provide
 1422 authentication. MTPSec can be used within the SS7 network
 1423 to achieve security of messages at MTP3 layer.

1424 4) *Use of secure protocols for SS7 over IP:* As it was
 1425 discussed earlier, voice and data have been merged and the SS7
 1426 protocol has been modified and integrated with other protocols
 1427 like SIGTRAN. This resulted in sending the SS7 messages
 1428 over IP. For these messages, secure protocols like IPSec [13]
 1429 should be used.

1430 5) *Deployment of Application Layer Firewall/ IDS/ Scan-
 1431 ners:* Application layer Firewall can be deployed to filter
 1432 out the SS7 MAP messages. Moreover, Intrusion Detection
 1433 system (IDS) [119] and scanners can also be used in addition
 1434 to the firewalls. These could be used in form of signature
 1435 detection or anomaly detection. To prevent exploitation of
 1436 known vulnerabilities, signature detection techniques will be
 1437 more useful. However, in future as more vulnerabilities will
 1438 be discovered and new attacks are expected to be disclosed,
 1439 anomaly detection technique will be more suitable. Firewall
 1440 can be deployed at STPs [47]. Most of the attacks target
 1441 STPs impersonating as other network/ roaming partner. Safe-
 1442 guarding the interconnections at STP is one of the most
 1443 important tasks. While communicating with STPs, the at-
 1444 tacker can exploit the inherent weakness of non-availability

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 implemented 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 algorithm 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. $x_1, x_2, x_3, \dots, x_n$. 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]:

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

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

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.

1549 **C. Artificial Neural Networks (ANN)**

1550 The idea of ANN has been derived from biological neural
 1551 networks. The purpose of ANN is to replicate the function-
 1552 ality of biological neural system in learning, correlating, and
 1553 improving with experience while solving complex problems.
 1554 ANN structure consists of multiple interconnected units for
 1555 data processing. These interconnected units are called artificial
 1556 neurons or nodes[133]. While designing ANNs, the goal of
 1557 designer is to adopt features of biological systems like learning
 1558 with experience, fault tolerance, parallel processing of the data,
 1559 adaptivity, and ability to generalize [134].

1560 *1) Structure of ANN:* As already described, ANNs consist
 1561 of neurons. Input neurons take input data, process it, and
 1562 forward results to the next layer [134]. Next layer does not
 1563 get input directly from the user program, rather it takes result
 1564 from previous layer of neurons. The output is given by the
 1565 output layer. Layers between input layer and output layer are
 1566 called hidden layers. At each neuron, inputs are multiplied
 1567 by a weight and then a mathematical function computes its
 1568 activation based on a threshold value set by the user. Multiple
 1569 neurons are grouped together to form ANN.

1570 If we take mathematical function as summation, a neuron
 1571 computes weighted sum of all input signals and generates an
 1572 output y based on threshold u [133].

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

- 1573 • x_j = Variable on j_{th} input
- 1574 • w_j = Variable on j_{th} Weight
- 1575 • θ = Unit step function at 0
- 1576 • u = Threshold value for activation of neuron

1577 Based on network architecture, ANNs are divided into two
 1578 main categories.

1579 *2) Recurrent or Feedback Networks:* These networks have
 1580 a memory of last state of network and are considered as
 1581 dynamic networks. They update their state continuously based
 1582 on their previous state until they achieve an equilibrium state.
 1583 When input is given, they compute output. The input is
 1584 modified with the output feedback and neuron enters into a
 1585 new state. Neurons have bi-directional connections between
 1586 them because of loops in the network.

1587 *3) Feed-Forward Networks:* In feed forward networks, neu-
 1588 rons have unidirectional connections between them i.e from
 1589 input to output and they can be considered as static networks.
 1590 Output of one layer only affects the next layer but not the
 1591 same layer. They are memory less networks as their output is
 1592 independent of previous network state. Persistence of previous
 1593 state to draw meaningful conclusion is very important while
 1594 dealing with complex problems. Non persistence of previous
 1595 state seems to be a major drawback of these networks.

1596 **D. Template for Rule Based Filtering**

1597 A proposed template which was implemented in python is
 1598 shown in Fig. 23. Simple rules in form of if-else statements
 1599 were defined and implemented. This template can be extended
 1600 to include other features and other type of MAP messages as

1601 per available dataset. Due to limitations of data set received
 1602 from simulator (limited number of features), machine learning
 1603 using other features block in Fig. 23 could not be used in the
 1604 experiment. However, in real SS7 data, it can be used.

1605 **E. Implementation Methodology**

1606 Open source SS7 attack simulator [51] was used to generate
 1607 the SS7 traffic. The simulator is built on open source JSS7
 1608 stack by Restcomm [135]. In addition to the JSS7 GUI and
 1609 Core Modes, it is built with following additional modes:

- 1610 • *1) Simple Mode:* It supports following attacks:
 1611 • Location tracking using Any Time Interrogation message
 1612 (location:ati).
- 1613 • Location tracking using Provide Subscriber Information
 1614 message (location:psi).
- 1615 • Intercepting SMS by stealing subscribers (intercept:sms).

1616 *2) Complex Mode:* In complex mode, simulator is built to
 1617 generate normal and attack data for a set of subscribers which
 1618 are passed as input string to the simulator.

1619 The details of the simulator and its working can be seen
 1620 in [48]-[50] Simulator was run in simple (SMS intercept)
 1621 and complex modes to generate a dataset that contained both
 1622 normal and attack packets. This data was captured on lo
 1623 interface of Wireshark.

1624 In case of real SS7 traffic, a network provider has a huge
 1625 amount of data for all subscribers. It is considered difficult
 1626 to process and use such a huge amount of data for anomaly
 1627 detection collectively for all subscribers. Concept of anomaly
 1628 detection for only one user given in [48]-[50] was followed.
 1629 Data needed to be pre-processed before using it for detection
 1630 of anomalies. Following important and relevant data attributes
 1631 were extracted from (Wireshark) pcap file into a csv file with
 1632 a terminal command:

1633 @ rootkali tshark -r input.pcap -Y gsm_map -T fields -e all
 1634 required fields > output.csv.

1635 Following fields were extracted:

- 1636 • Time of the MAP message.
- 1637 • Destination address (dpc).
- 1638 • Source address (opc).
- 1639 • Length of MAP message.
- 1640 • Type of MAP message.
- 1641 • Subscriber IMSI.
- 1642 • SCCP details.
- 1643 • Area from which message generation is simulated
- 1644 • Location Area Code.

1645 This dataset contained data for a set of subscribers. With
 1646 simple grep command from terminal, all data of one particular
 1647 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)

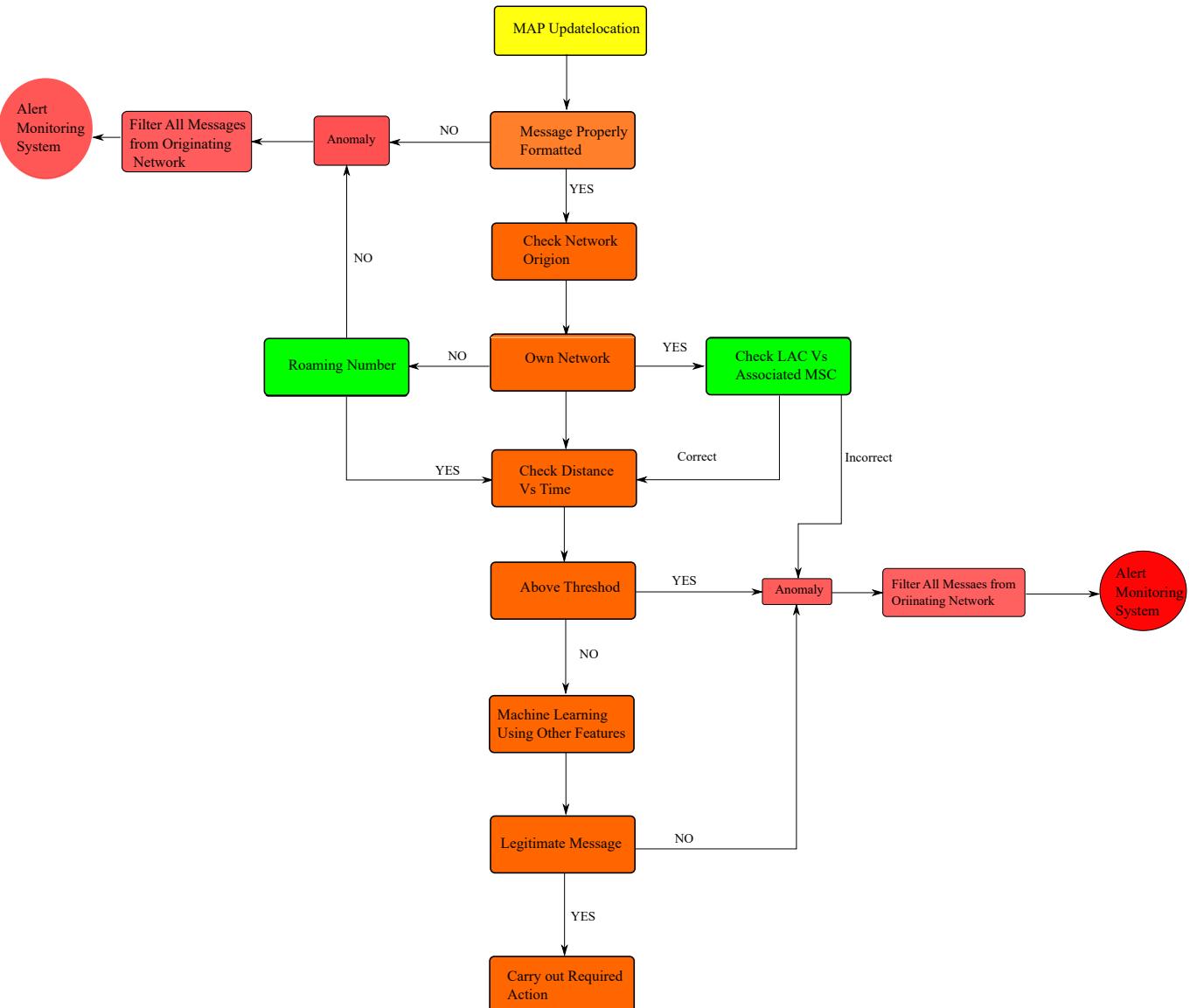


Fig. 23. Template for rule based filtering



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.

1648 subscriber. The separated data contained normal and attack
 1649 traffic for a particular subscriber. Again grep command was
 1650 used to separate MAP Update Location messages for that
 1651 subscriber. Open source python scripts are also available to
 1652 preprocess the data for machine learning [136]. The received

dataset contained normal and attack MAP Update Location
 1653 messages for a single subscriber. Different features of this
 1654 dataset have been used for machine learning as under:
 1655

- Time difference between MAP update location messages
 1656 is used to check distance travelled vs time taken. Time of
 1657

- 1658 the movement of subscriber is also used in training the
1659 neural network.
 1660 • Local Area Codes (LACs) is used to model normal
1661 behaviour of the user assuming that user do not travel out
1662 of a particular area in normal circumstances. Simulator
1663 provides only a limited set of LACs. Due to which, this
1664 feature is not directly used for machine learning. Here,
1665 movements between different LACs is used to define
1666 normal behaviour of the subscriber. However in real
1667 time data, this feature can be very useful for modelling
1668 subscriber's movements.
 1669 • Length of the MAP messages in bytes and format of
1670 received message is used to check malicious messages.
1671 This feature is used on the assumption that the attacker
1672 crafts attack packets which slightly vary from original
1673 format/size[48] of MAP update message used by the
1674 service provider.
 1675 • Correlation of MSC addresses vs corresponding LACs
1676 can be used for detection of an attack packet received
1677 from own network as it will be easy to check received
1678 message MSC address and present LAC of the user.
1679 Simulator provides a very limited set of these addresses
1680 due to which this feature is not used with this data set. In
1681 real time, if a network operator can compare LAC & MSC
1682 pair received, with those actually implemented within a
1683 network, it will give a very good indication of an attack
1684 assuming an attacker does not know addresses of MSCs.

1685 Dataset received from the simulator contains only a limited
1686 number of LACs; where a user moves, and from where attack
1687 packets are created. These limited LACs cannot be used for
1688 defining the user profile to detect anomalies directly. However
1689 movements of a selected user from one LAC to another
1690 LAC are converted into distance travelled. Distance is used
1691 to compare with time elapsed since last message as one of the
1692 features.

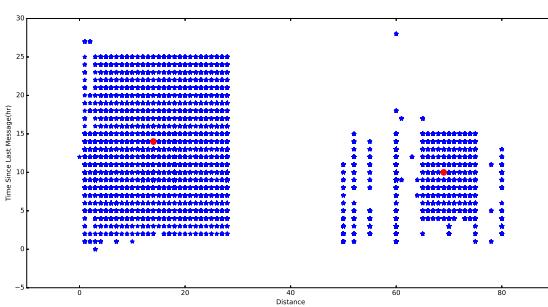
1693 Let us say our selected subscriber normally moves in the
1694 LAC₁ through LAC_n as shown in Fig. 24. The distance
1695 between LACs in which a user normally moves is kept less
1696 than X km where X = x₁, x₂, x₃.....x_n.
 1697 The user moves from LAC₁ to LAC₂ and covers distances x₁₂
1698 Distance(LAC₁, LAC₂) = x₁₂
 1699 User moves from LAC₂ to LAC₃ and covers distances x₂₃

$$\begin{aligned} \text{Distance}(LAC_2, LAC_3) &= x_{23} & 1700 \\ \text{The user moves from } LAC_1 \text{ to } LAC_3 \text{ and covers distances } x_{13} & & 1701 \\ \text{Distance}(LAC_1, LAC_3) &= x_{13} & 1702 \\ . & & 1703 \\ . & & 1704 \\ . & & 1705 \\ . & & 1706 \\ \text{Distance}(LAC_1, LAC_n) &= x_{1n} & 1707 \end{aligned}$$

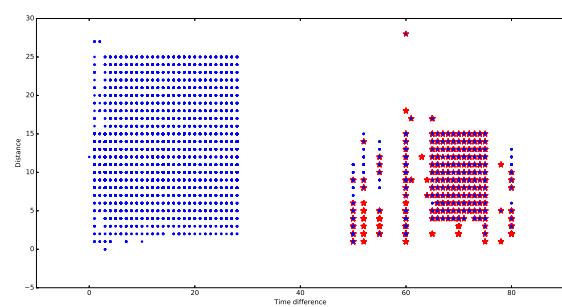
Case 1

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

Problem in This Method: We assume a user was in LAC₁ 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 LAC₁ to LAC_{unknown} will be converted into distance y₁ 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 LAC₂ and updates her position via MAP Update Location message. The distance from LAC_{unknown} to LAC₂ will be translated into y₂ ($y_2 > X$). This will be almost same distance as y₁. 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

1739 *Proposed Solution(Case 2)*

1740 Let us consider distance from a user normal profile and an
 1741 unknown LAC outside the user normal profile is not equal
 1742 in both directions. Distance from normal profile to a new
 1743 area is kept greater than distance between any LAC within
 1744 the user normal profile but distance from an area outside the
 1745 user normal profile back to the user profile is kept equal to
 1746 normal distance used between LACs inside the user profile.

$$1747 \text{Distance}(LAC_{1,2,3,\dots,n}, LAC_{\text{unknown}})$$

$$1748 \neq \text{Distance}(LAC_{\text{unknown}}, LAC_{1,2,3,\dots,n})$$

$$1749 \text{Distance}(LAC_{1,2,3,\dots,n}, LAC_{\text{unknown}}) = y (y > X)$$

$$1750 \text{Distance}(LAC_{\text{unknown}}, LAC_{1,2,3,\dots,n}) = X$$

1751 In above scenario, when a user moves to LAC_2 the distance
 1752 will be translated to normal distance and it will not be
 1753 considered an anomaly. Again the same problem exists here,
 1754 if user moves away from normal profile area into a new area
 1755 it will again be considered an anomaly.

1756 *F. Results*

1757 After obtaining a dataset of 35640 sample messages which
 1758 contained 2248 malicious packets, following features were
 1759 selected for machine learning as recommended by [48]-[50]:

- 1760 • Distance travelled by a user.
- 1761 • Time taken to cover the distance.
- 1762 • Format of message/ Byte length. This feature can only
 1763 be used if an attacker sends messages which has higher
 1764 or lower number of bytes than a normal message of the
 1765 same type or if message is not properly formatted. If
 1766 message is properly formatted then this feature will give
 1767 no indication of an attack or malicious intent.
- 1768 • Originator address (OPC). MAP update location message
 1769 can be originated from own network or from a roaming
 1770 partner. It can be filtered on the basis of OPC if it is other
 1771 than own network or a roaming partner.
- 1772 • Frequency of MAP Update messages.

1773 In case 1, K-Means Clustering Algorithm detected 4390
 1774 packets as anomalies. All the actual malicious packets were
 1775 detected correctly and 2142 false positives were generated.
 1776 These 4390 packets were assigned same cluster as shown in
 1777 Fig. 25a. As explained in case 1, the distance was almost same
 1778 for two packets i.e the attack packet and the immediate packet
 1779 after the attack packet. Attack packet was sent by the attacker
 1780 from LAC_{unknown} . It was translated into abnormal distance.
 1781 However, when the user moved to a new location and her
 1782 location was updated, again distance from LAC_{unknown} to the
 1783 user normal profile was translated to abnormal distance. The
 1784 algorithm assigned same cluster to both the packets as shown
 1785 in Fig. 25a, based on the distance involved. Cluster on right
 1786 side of Fig. 25a show both types of packets were assigned
 1787 same cluster. In case 2, K-Means Clustering algorithm detected
 1788 2987 packets as anomalies. All the actual anomalies were
 1789 detected correctly and 739 false positives were generated as
 1790 compared to 2142 anomalies in case 1. The reduction in false
 1791 positives observed because in case 2 distance for two packets,
 1792 attack packet and immediate (legitimate) packet after attack
 1793 packet was not same. False positives in this case were due to
 1794 other features of the data set being used.

1795 Rule based filtering detected 3365 packets as anomalies with
 1796 1117 false positives in both the cases because of nature of
 1797 artificial data. Two dimensional plots of K-means clustering
 1798 and Rule based filtering for case 1 are shown in Fig. 25a and
 1799 25b. In Fig. 25b red dots indicate attack packets and blue
 1800 dots indicate normal packets. In rule based filtering, in cluster
 1801 on right side of Fig. 25b, two packets i.e the attack packet
 1802 and the immediate packet after the attack packet can be seen
 1803 with red and blue dots respectively. The attack packet sent by
 1804 the attacker was detected as attack packet and is shown in red
 1805 colour and immediate legitimate packet after attack packet due
 1806 to user movement was detected as normal packet. Rule based
 1807 filtering could not detect attack packets which were sent within
 1808 the user normal profile from the attacker.

1809 ANNs were applied on a reduced dataset of 10945 samples
 1810 due to requirement of labels. Results are summarized in table
 1811 VI.

1812 From results obtained in table VI, it can be concluded that
 1813 for real SS7 data, rule based filtering should be implemented
 1814 for all SS7 MAP messages at first defensive layer. As we
 1815 have seen, machine learning can also be implemented with
 1816 a considerable success, at second defensive layer appropriate
 1817 machine learning algorithm should be applied with carefully
 1818 chosen features from user data.

1819 Machine learning can be used for detection of all types of
 1820 anomalies in the SS7 network. It has the potential to detect
 1821 zero day attacks; however, it may miss some valid attacks and
 1822 may give more false alarms as compared to rule based filtering.

1823 Rule based filtering can be used for filtering of particular
 1824 types of messages with greater accuracy as compared to
 1825 machine learning techniques. It is expected to generate less
 1826 false alarms as compared to machine learning techniques.
 1827 There are certain limitations with rule based filtering which
 1828 include each type of the SS7 message will need a separate rule
 1829 based template to detect attacks. For designing these templates,
 1830 greater understanding of internal working of the SS7 network
 1831 is needed. Moreover, it is not expected to detect zero day
 1832 attacks.

1833 *VII. FUTURE WORK*

1834 Research on impact of the SS7 vulnerabilities on LTE/4G
 1835 and 5G networks due to backward compatibility remains an
 1836 open area of research. Attacks on diameter protocol has been
 1837 described as an evolution of the SS7-based attacks [13] which
 1838 needs be further studied to find out the extent of compromise
 1839 to the users private parameters possible with these attacks.

1840 Development of filtering techniques for MAP SRI and MAP
 1841 SRI SM messages is an open area of research because these
 1842 messages are used for legitimate purpose and can be origi-
 1843 nated from any network. Techniques to detect such malicious
 1844 messages remain a challenge.

1845 In case of real SS7 traffic, a network provider has a huge
 1846 amount of data for all subscribers. One of the challenges is to
 1847 process such a huge data simultaneously for online detection
 1848 of attacks on the SS7 networks. To process such a huge data
 1849 feasibility of existing tools/ techniques need to be ascertained.
 1850 Moreover, development of new tools/ techniques for efficient
 1851 processing of huge data is also an open challenge.

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

1852 Access to real data of SS7 remains the main limiting factor
 1853 for academia due to privacy issues. However, development of
 1854 a fully virtual SS7 network/ test bed needs to be studied to
 1855 facilitate future research on this topic.

1856 The SS7 attack simulator can be considered a good initial
 1857 step towards development of a fully functioning SS7 attack
 1858 simulator. As a future work its functionality can be extended
 1859 to include maximum SS7 MAP messages and all publicly
 1860 disclosed attacks. In this work only one type of MAP message
 1861 (MAP update location message) was focused keeping in mind
 1862 the capabilities of simulator. In future work, scope of detection
 1863 of malicious MAP messages can also be increased to include
 1864 all types of attack messages. Implementation of more machine
 1865 learning techniques can also be investigated to check their
 1866 feasibility. Moreover rule based filtering templates can be
 1867 defined and implemented for all types of MAP messages
 1868 which can be exploited by the attackers. In real SS7 data,
 1869 both techniques (rule based filtering and machine learning) are
 1870 recommended to be checked simultaneously for determining
 1871 the accuracy of proposed method.

VIII. CONCLUSION

1872 Telecommunication networks have gained a significant popularity
 1873 due to various factors. Signalling system is used for management
 1874 of calls in telecommunication systems. The SS7 was designed
 1875 in 1970s on the concept of a boundary walled technology. With
 1876 the passage of time as the boundary walls of the SS7 network
 1877 expanded, it has become increasingly open to more service providers.
 1878 This expansion has resulted in increased interfaces and developed certain threats to the
 1879 privacy of the subscribers. In this paper, methods to enter
 1880 into the SS7 network have been explained due to lack of
 1881 inherent security controls. It has been explained in the paper
 1882 that location tracking of a subscriber is possible at MSC level
 1883 which can be narrowed down to a smaller area. Possibility of
 1884 location tracking to a cell level and accurate location tracking
 1885 has also been explained. Cases for interception, storage and
 1886 modification of calls and short messages have been described.
 1887 Possibility to create DoS, sending spam messages and carrying
 1888 out fraudulent activities by the attackers has been presented.
 1889 Different options for defenses against exploitation of the SS7
 1890 vulnerabilities have been presented. A machine learning based
 1891 1892

1893 framework to detect anomalies in the SS7 network has been
 1894 presented and its results have been compared with rule based
 1895 filtering on simulated SS7 data set.

ACKNOWLEDGEMENT

1896 This research is supported by the Higher Education Com-
 1897 mission (HEC), Pakistan through its initiative of National
 1898 Center for Cyber Security for the affiliated lab National Cyber
 1899 Security Auditing and Evaluation Lab (NCSAEL), Grant No:
 1900 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. Sheno, "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.

- 1942 [16] H. Kaaranen, S. Naghian, L. Laitinen, A. Ahtiainen, and V. Niemi,
1943 "UMTS Networks: Architecture, Mobility and Services." New York:
1944 Wiley, 2001.
- 1945 [17] ETSI, TS. "136 101 V10. 3.0 (2011-06) LTE.Evolved universal ter-
1946 resterrial radio access (E-UTRA)."
- 1947 [18] Verint Skylock product brochure: [Online]. Available:
1948 [http://apps.washingtonpost.com/g/page/business/
1949 skylock-product-description-2013/1276/](http://apps.washingtonpost.com/g/page/business/skylock-product-description-2013/1276/)
- 1950 [19] Defentek Infiltrator product brochure: [Online]. Available:
1951 [https://assets.documentcloud.org/documents/810690/263-defentek-
1953 brochure-infiltrator.pdf](https://assets.documentcloud.org/documents/810690/263-defentek-
1952 brochure-infiltrator.pdf)
- 1954 [20] S. Gibbs, "US congressman calls for investigation into vulnerability
1955 that lets hackers spy on every phone." The Guardian, 2016. [On-
1956 line]. Available: [https://www.theguardian.com/technology/2016/apr/19/
1957 ss7-hack-us-congressman-calls-texts-location-snooping](https://www.theguardian.com/technology/2016/apr/19/ss7-hack-us-congressman-calls-texts-location-snooping)
- 1958 [21] A. Gellman and A. Gellman, "New documents show how the NSA
1959 infers relationships based on mobile location data." Washington Post,
1960 2013. [Online]. Available: <https://goo.gl/CmIzn>
- 1961 [22] C. McDaid, "Can They Hear You Now? Hacking Team
1962 & SS7 | AdaptiveMobile." [Adaptivemobile.com](http://www.adaptivemobile.com), 2015.
1963 [Online]. Available: [http://www.adaptivemobile.com/blog/
can-they-hear-you-now-hacking-team-ss7](http://www.adaptivemobile.com/blog/can-they-hear-you-now-hacking-team-ss7)
- 1964 [23] "Positive Technologies - vulnerability assessment, compliance manage-
1965 ment and threat analysis solutions." Ptsecurity.com. [Online]. Available:
1966 <https://www.ptsecurity.com/ww-en/>
- 1967 [24] B. Goodwin, "Security flaw exposes billions of mobile phone users
1968 to eavesdropping." Computer Weekly, August 14 2015, [Online]. Available
1969 [http://www.computerweekly.com/news/4500251756/
1970 Security-flaw-exposes-billions-of-mobile-phone-users-to-eavesdropping](http://www.computerweekly.com/news/4500251756/Security-flaw-exposes-billions-of-mobile-phone-users-to-eavesdropping)
- 1971 [25] C. Timberg, "German researchers discover a flaw that
1972 could let anyone listen to your cell calls." The Wash-
1973 ington Post, December 18 2014, [Online]. Available:
1974 [https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/
1975 german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-\
1976 your-cell-calls-and-read-your-texts/?utm_term=.de15e5842bf](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=.de15e5842bf)
- 1977 [26] B. Clark, "Watch hackers hijack WhatsApp and Telegram accounts
1978 using known telecom flaw." June 1 2016, [Online]. Available <http://thenextweb.com/insider/2016/06/01/watch-hackers-hijack-whatsapp>
- 1979 [27] P1 Security. December 2014. "SS7map: SS7 Networks Exposure."
1980 [Online]. Available: <https://ss7map.p1sec.com/>
- 1981 [28] G. Lorenz, J. Keller, G. Manes, J. Hale and S. Shenoi. "Public tele-
1982 phone network vulnerabilities." In Database and Application Security
1983 XV, pp. 151-164. Springer, Boston, MA, 2002.
- 1984 [29] C. Xenakis, and L. Merakos. "Security Architecture Standardization
1985 and Services in UMTS." Proc. Mobile Venue, pp 585-592, 2002.
- 1986 [30] H. Sengar, R. Dantu, and D. Wijesekera, "Securing VoIP and PSTN
1987 from integrated signaling network vulnerabilities." 1st IEEE workshop
1988 on VoIP Management and Security (VoIP MaSe), Vancouver, Canada,
1989 April 2006.
- 1990 [31] C. Xenakis and L. Merakos, "Security Architecture Standardization and
1991 Services in UMTS." Proc. Mobile Venue, pp 585-592, (2002).
- 1992 [32] H. Sengar, R. Dantu, D. Wijesekera, and S. Jajodia. "SS7 over IP:
1993 Signaling internetworking vulnerabilities." IEEE Network 20 (6), pp.
1994 32-41, November 2006.
- 1995 [33] V. Chandola, A. Banerjee, V. Kumar, "Anomaly detection: A survey."
1996 ACM computing surveys (CSUR)41(3), July 2009.
- 1997 [34] P. Langlois, "SCTPscan-Finding entry points to SS7 networks &
1998 telecommunication backbones." In BlackHat Convention (BH), Europe
1999 2007.
- 2000 [35] "Black Hat", [Online]. Available: <http://blackhat.com/>
- 2001 [36] T. Engel, "Locating Mobile Phones using Signaling System#7." In
2002 25th Chaos Communication Congress 25C3 2008, [http://berlin.ccc.de/
2003 ~tobias/25c3-locating-mobile-phones.pdf](http://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf)
- 2004 [37] K. Kotapati, "Assessing security of mobile telecommunication net-
2005 works." (2008).
- 2006 [38] K. Kotapati, P. Liu, and T. F. Porta. "Evaluating MAPSec by marking
2007 attack graphs." Wireless Networks 15(8) pp 1042-1058, Springer, 2009.
- 2008 [39] J. Lingling and M. Hong, "New Trends of Attack and Prevention
2009 Technologies in Telecommunication." In Information Technology and
2010 Applications (IFITA'09) 1, pp. 80-82. IEEE, 2009.
- 2011 [40] A. Xinyuan, J. Chen, Y. Liu, X. Wei, and T. Xu, "A defense method
2012 based on improved MTP3 message discrimination in SS7 network." In
2013 Natural Computation (ICNC), Seventh International Conference (2),
2014 pp. 711-715. IEEE, 2011.
- 2015 [41] S. Mjølsnes and J. K. Tsay, "Computational security analysis of
2016 the UMTS and LTE authentication and key agreement protocols." 6th
2017 International Conference on Mathematical Methods, Models and
2018
- 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
2030 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
2031 Communication Backend." Master's thesis, University of Tartu, 2015.
- [48] K. Jensen. "Improving SST Security Using Machine Learning Tech-
2032 niques." Master's thesis, Norwegian University of Science and Tech-
2033 nology, 2016.
- [49] K. Jensen, T.Van Do, H.T Nguyen, A. Arnes, "Better protection of SS7
2034 using machine learning techniques." In 6th International Conference on
2035 IT Convergence and Security (ICITCS) (2016).
- [50] K. Jensen, T.Van Do, H.T Nguyen, A. Arnes, "A big data analytics
2036 approach to combat telecommunication vulnerabilities" Cluster Com-
2037 puting 20(3), pp.2363-2374, 2017
- [51] "SS7 Attack Simulator based on RestComm's jss7." [Online]. Avail-
2038 able: <https://github.com/polariking/jss7-attack-simulator>
- [52] S. Holtmanns, S. P. Rao, and I. Oliver, "User location tracking attacks
2039 for LTE networks using the interworking functionality." In 2016 IFIP
2040 Networking Conference (IFIP Networking) and Workshops, pp. 315-
2041 322, May 2016.
- [53] M. Hamdi et al, "Voice Service Interworking for PSTN and IP
2042 Networks." IEEE Commun. Mag, pp. 104-11,1999.
- [54] M. Savadatti and D. Sharma, "SS7 Network and Its Vulnerabilities:
2043 An Elementary Review." Imperial Journal of Interdisciplinary Research
2044 (IJIR)3(3), pp. 912-916, 2017.
- [55] S. Puzankov, "Stealthy SS7 Attacks", Journal of ICT Standardization
2045 5(1), pp. 39-52, 2017.
- [56] N. Andrews, "CAN I GET YOUR DIGITS? ILLEGAL ACQUISITION
2046 OF WIRELESS PHONE NUMBERS FOR SIM-SWAP ATTACKS
2047 AND WIRELESS PROVIDER LIABILITY, 16 Nw. J. Tech. & Intell.
2048 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
2049 communication user data." Sci China Inf Sci, 2018, 61(10): 109303,
2050 <https://doi.org/10.1007/s11432-017-9428-6>
- [58] L. Abdelrazek and M. A Azer. "SigPloit: A New Signaling Exploitation
2051 Framework." In Tenth International Conference on Ubiquitous and
2052 Future Networks (ICUFN), pp. 481-486. IEEE, 2018.
- [59] T. Qasim, M. Hanif Durad, A. Khan, F. Nazir, and T. Qasim. "Detection
2053 of signaling system 7 attack in network function virtualization using
2054 machine learning." In fifteenth International Bhurban Conference on
2055 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
2056 to SMS on Android." In International Conference on Intelligent Com-
2057 puting & Optimization, pp. 505-514. Springer, Cham, 2018.
- [61] Prof. J. Kulubi, "Glossary of terms & standards used in telecommuni-
2058 cation systems." [Online]. Available: http://eti2506.elimu.net/Glossary/Glossary_Telecom.html
- [62] O. Kong Chung, "SS7 OPNET simulation Signaling System No.7,
2059 (SS7) network interfaces." Master's Thesis, Naval Postgraduate School,
2060 California, 2000.
- [63] J. Van Bosse and F. Devetak, "Signaling in telecommunication net-
2061 works." Hoboken, N.J.: Wiley-Interscience, 2007.
- [64] J. Van Bosse and F. Devetak, 'Signaling in telecommunication net-
2062 works'. Hoboken, N.J: Wiley-Interscience, 2007, Chapter7 pp (157-
2063 166).
- [65] Performance Technologies, "Tutorials on Signaling System 7 (SS7)." [Online].
2064 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
2065 Signalling System No. 7 Networks." In Second IEEE symposium on
2066 Computers and Communications, pp. 109-113, 1997.
- [67] CAP, CAMEL Application Part. "TS-3GA-29.078 (Rel4) v4. 4.0 Customised
2067 Applications for Mobile network Enhanced Logic (CAMEL);
2068 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://technocrateservices.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. Bondoni, 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, "Unlocking 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. Morneau, 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.

- 2248 [128] N. Williams, S. Zander and G. Armitage, "A preliminary performance
2249 comparison of five machine learning algorithms for practical IP traffic
2250 flow classification" ACM SIGCOMM Computer Communication Review 36(5), pp.5-16, 2006.
2251
2252 [129] P. Berkhin, "A survey of clustering data mining techniques." Grouping
2253 Multidimensional Data, pp. 25-71, Springer, Berlin, Heidelberg, 2006.
2254
2255 [130] A. Trevino, "Introduction to K-means Clustering" Online blog. Available:
2256 <https://www.datascience.com/blog/k-means-clustering?>
2257
2258 [131] Euclidean distance, Wikipedia [Online]. Available: https://en.wikipedia.org/wiki/Euclidean_distance
2259
2260 [132] corvasto/Simple-k-Means-Clustering-Python, <https://github.com/corvasto/Simple-k-Means-Clustering-Python>
2261
2262 [133] I. A. Basheer and M. Hajmeer, "Artificial neural networks: fundamentals,
2263 computing, design, and application." Journal of microbiological methods 43(1), pp. 3-31, 2000.
2264
2265 [134] A.K Jain, J. Mao and K.M Mohiuddin, " Artificial neural networks: A
2266 tutorial." Computer 29(3), pp.31-44, 1996.
2267
2268 [135] Restcomm, "jss7 GitHub Repository." 2015, [Online]. Available: <https://github.com/Mobicents/jss7/>
2269
2270 [136] K. Jensen, "SS7 Preprocessing GitHub Repository." 2016, [Online].
2271 Available: <https://github.com/polariking/ss7-preprocessing>
2272
2273 [137] Vacca, John R. Computer and information security handbook. 2012.
2274 Chapter 17
2275
2276
2277
2278
2279
2280
2281



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 of 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.



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.



(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 of 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.



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. 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.

2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382



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 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.