Investigating GSM Control Channels with RTL-SDR and GNU Radio

Conference Paper · March 2016

DOI: 10.1109/WiSPNET.2016.7566288

3 authors, including:

Khyati P Vachhani
The MathWorks, Inc
13 PUBLICATIONS **67** CITATIONS

SEE PROFILE

This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2016 conference.

Investigating GSM Control Channels with RTL-SDR and GNU Radio

Deepak Vohra
Student, Electrical Dept.
Nirma University,
Ahmedabad, India
dvohra.93@gmail.com

Arusha Dubey
Student, Electrical Dept.
Nirma University,
Ahmedabad, India
arusha.dubey31@gmail.com

Khyati Vachhhani
Assistant Professor, Electrical Dept.
Nirma University,
Ahmedabad, India
khyati.vachhani@nirmauni.ac.in

***Abstract*—This paper focuses on the compliance of publicly available specifications of Global System for Mobile communication (GSM) with the extremely closed GSM industry with the help of RTL-SDR, GNU Radio and Wireshark. GNU Radio is a free and open software which enables the translation of real-world systems to programmable flow graphs. GSM, together with other technologies, is part of the evolution of wireless mobile telecommunications. Hence, verification of GSM working is of crucial importance. During this paper, Control channel information like the bandwidth for specific network providers was reckoned, along with the IMSI number and ARFCN channel in use by mobile device of the respective network. It was also noted that observed cell towers used both frequency hopping and encryption. The channel information thus obtained provides efficient techniques for the detection of spectrum holes providing high spectral resolution capability.**

***Index Terms*—GSM,SDR,RTL-SDR,GNU Radio,Wireshark, Common Control Channels**

I. Introduction

The mobile communication has undergone a tremendous growth and has influenced different spheres of human race. In 2015, the number of mobile users has nearly reached to 6 billion users amongst which 4 billion users are using Global System for Mobile Communication (GSM) around the globe. Global System for Mobile Communication [1], a second-generation cellular system is the first cellular system to identify digital modulation along with network level architecture and its related services. GSM has observed spectacular refinement leading to various versions like GSM1800, HSCSD (High Speed Circuit Switched Data), EDGE (Enhanced Data rates for GSM Evolution), and GPRS (General Packet Radio Service) and continued to 3G systems like Universal Mobile Telecommunication Systems (UMTS). With the knowledge that GSM consists of several inherent security flaws, 3G systems like UMTS [2] were able to address these security flaws methodically. Nevertheless, the traditional GSM network which fails to resist several security flaws is still followed by many developing countries around the globe. Soon after its implementation, GSM was found unprotected to eavesdropping attacks [3]. Since there is no authentication required between Base Transceiver Station (BTS) and Mobile Station (MS) and network operators are not impelled on using encryption in public land mobile network (PLMN), the entire system becomes ineffectual in providing necessary requirements in terms of privacy and security of the subscriber. This results in possible active or passive attacks on GSM networks. Despite the fact that highly resourceful GSM intercepting hardwares are present, procurement and endmost approval of such hardware is in the hands of government agencies only. Ultimately, this obstructs the analysis and testing of GSM infrastructure. With the enhancement of several open-source softwares viz GNU Radio, Airprobe, Wireshark and Openbts along with reconfigurable-reprogrammable hardwares viz Software Defined Radio [4], it is now possible to analyze the GSM network for more robust security and efficiency. This paper focuses on analysis of GSM downlink traffic on Um interface that is present between Base Transceiver Station (BTS) and Mobile Station (MS).

The paper is organized as follows: Section 2 describes the theoretical background of GSM system architecture and network Architecture with necessary block diagrams. Section 3 discusses the open-source software tools and hardware used to capture downlink packet data. Section 4 describes analysis of GSM protocol stack by amalgamation of RTL-SDR, GNU Radio and Wireshark. In Section 5, the results captured by Wireshark and GNU Radio are analysed and verified with the designated test phone. The future scope on security enhancement and more research required on software front is discussed in section 6. Lastly, the paper ends with conclusion.

II. Theoretical background of GSM

A. GSM System Architecture

The GSM network is divided into three major sub-systems, being the Base Station Subsystem (BSS), Network and Switching Subsystem (NSS) and the Operation Support Subsystem (OSS) [5]. BSS is sometimes also referred to as the GSM Access Network (AN) while NSS is conveniently called the GSM Core Network (CN). The Mobile Station (MS) is a device of utility to the subscriber which is considered to be a part of the BSS and is used to access the services provided by the mobile network. The BSS, responsible for management of radio interface between mobile stations and all other subsystems, consists of several Base Transceiver Stations (BTS) controlled by Base Station Controller (BSC). Another

978-1-4673-9338-6/16/$31.00

important part of the BSS is transcoder/rate adaption unit (TRAU) which performs speech encoding and decoding and rate adaptation during data transmission. The NSS performs key functions of the network such as call control, mobility management, routing and switching apart from subscription information and service provision based on this information. It also manages communication with other networks such as Integrated Services for Digital Network (ISDN) and Public Switched Telephone Network (PSTN). Within the GSM NSS, the permanent master database is stored in the Home Location Register (HLR) and the temporary database of the subscribers currently visiting the mobile network in the Visitor Location Register (VLR).

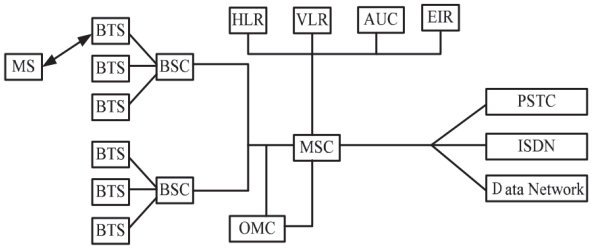

Fig. 1: GSM System Architecture [5]

The subscriber authentication unit is labelled as the Authentication Centre (AuC) while the handset verification is assigned to the Equipment Identity Register (EIR). The Mobile service switching centre (MSC) controls several BSCs and coordinates call set-up to and from GSM users. The three major areas of OSS are namely the network operation and maintenance functions, subscription management i.e. charging and billing, and mobile equipment management. These tasks are carried out under the main unit of OSS - the Operational and Maintenance Centre (OMC). Mobile Equipment (ME) and Subscriber Identity Module (SIM) are the components of MS. SIM are a smart cards containing multiple application software modules for secure identification of the subscriber. It stores the permanent identity of the user called the International Mobile Subscriber Identity (IMSI) and shared secret key. It can be easily inserted in the ME. The radio interface between MSC and BSC is called A Interface. The interface between BSC and BTS is the A-bis interface whereas the interface between MS and BTS is called Um interface.

B. GSM Network Architecture

It is crucial in a mobile network to have an efficiently designed structure for routing the calls correctly. It is therefore a challenging task due to the mobility of the subscribers. A GSM network is partitioned into the following areas:

- GSM service area;
- PLMN service area;
- MSC service area;
- Location area (LA);
- Cells.

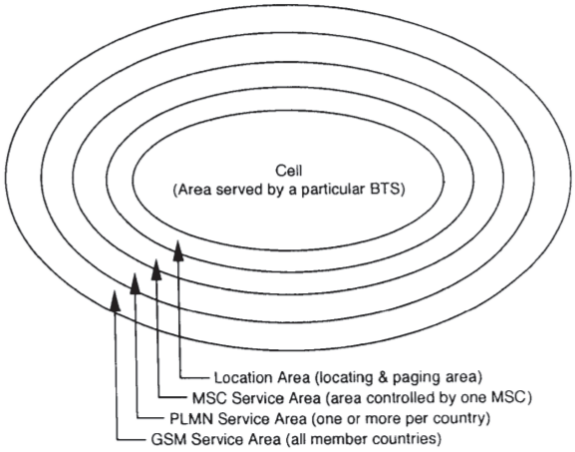

Fig. 2: GSM System Architecture [6]

The combined area of all the countries using GSM services constitutes the GSM service area [6]. A country is further divided into several PLMN service areas depending upon its size. A PLMN has several MSC/VLR service areas. A gateway MSC routes all the incoming calls in a PLMN network and makes inter-connections for calls between PLMNs. They route the incoming calls to the desired MSC within the MSC area wherein a subscribed is located. The VLR uniquely identifies the MS and is associated with the MSC. A single MSC service area has many LA. The GSM system uses LA to identify an active subscriber. While roaming in a LA, the MS need not update its location to the MSC/VLR. The LA can be identified by the system using the Location Area Identity (LAI). Finally, a LA is partitioned into several cells. A cell is an identity served by one BTS. The Base Station identification Code (BSIC) differentiates one cell from another.

III. Hardware-Software Suite

A. Sotware Defined Radio

Software Defined Radio (SDR) is defined as a radio communication system wherein some or all physical layers can be defined as software modules. The Radio Frequency (RF) signal generated or captured by the SDR is programmed by softwares, greatly reducing hardware complexity [7]. For

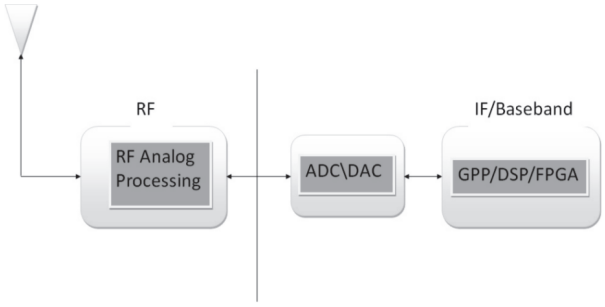

Fig. 3: Block Diagram of Software Defined Radio[7]

executing communication experiments on SDR, hardware like

Universal Software Radio Peripheral (USRP) [8] or Realtek-Software Defined Radio (RTL-SDR) can be used. USRP is a transceiver developed by Ettus Research and National Instruments. It turns a host computer into a wireless prototyping system. While USRP however is costly, RTL-SDR is a low cost alternative. RTL-SDR is a cost effective software defined radio that uses a DVB-T TV tuner dongle based on the RTL2832U chipset. It is also often referred to as RTL2832U, DVB-T SDR, RTL dongle or the $20 Software Defined Radio.

B. GNU Radio

GNU Radio is an open source software tool kit that enables building of a Software Defined Radio. The prime advantage obtained by GNU Radio is by creating different radio devices on a single USRP board. Different functionalities like modulation, demodulation, filtering, encoding, decoding, source coding, channel coding etc. are provided as software codes [9]. The advantage of implementing functionalities as software modules is that it provides a high degree and ease of reconfigurability property to SDR. One of the helpful attributes accepted by GNU Radio is the spectrum analyzing tool which can be useful in detecting the carrier frequency of a BTS. Also in conjunction with Airprobe tool, collective broadcast messages from the BTS can be acquired.

C. Wireshark

Wireshark, previously known as Ethereal, is a packet analyser. It is an efficient way to learn exactly how the network protocols work. It observes the messages exchanged between executing protocol entities and displays the content of various protocol fields in these captured messages.

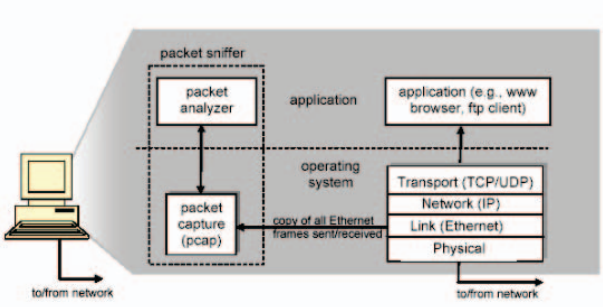

Fig. 4: Wireshark-A protocol Analyzer

A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself [10]. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a copy of packets that are sent or received from and by application and protocols executing on your machine. Network professionals also use Wireshark to troubleshoot networking problems.

IV. Analysis of Downlink GSM Traffic

GSM-900, also called as P-GSM, has a frequency spectrum of 25 MHz bandwidth which is further divided into 124 carrier frequencies spaced at 200 KHz. These carrier frequencies are termed as Absolute Radio Frequency Channel Number (ARFCN). Similarly, for GSM-1800, known as E-GSM, with a frequency spectrum of 75 MHz bandwidth, 374 ARFCNs are obtained when regularly spaced at 200 KHz.

Due to lack of inexpensive hardware and complex signaling present, remarkable attempts were not carried out for acquisition and decoding of downlink GSM traffic. Nonetheless, the recent existence of open-source tools viz SDR, GNU Radio, Airprobe and Wireshark has changed the outlook remarkably. Several versatile and inexpensive SDRs have become prominent in investigating the Radio Frequency (RF) spectrum. Some of these are RTL-SDR, USRP, FUNcube Dongle etc. Instead of USRP, RTL-SDR is used to further investigate the GSM downlink traffic.

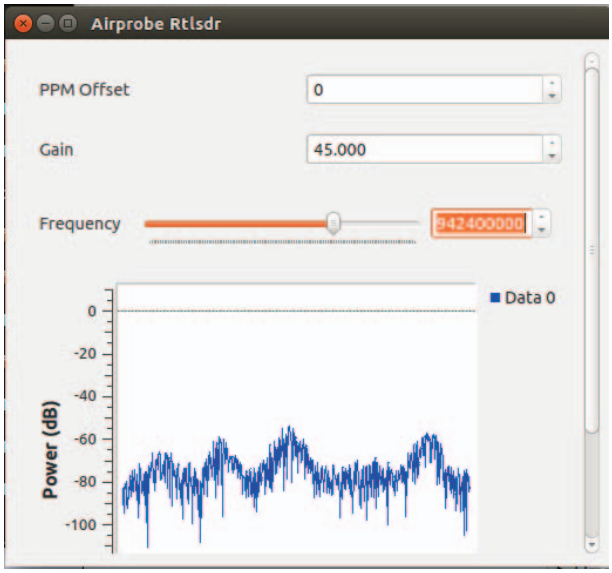

Fig. 5: P-GSM spectrum Caputred with GNU Radio & Airprobe

At software front, GNU Radio and Airprobe in synchrony with open-source protocol analyser Wireshark were used to capture and analyse the GSM downlink traffic as shown in Fig. 5. The analysis can be explicitly done using Wireshark wherein packet data in form of octet bits of various GSM logical channels can be obtained. Then after, RTL-SDR instead of USRP can be used for capturing the raw GSM frames from Um interface. The GSM frames are captured using RTL-SDR in conjunction with GNU Radio and the corresponding data is stored in a file named as .cfile.

Using the following equations and ARFCN channel number (n) as obtained in Wireshark, the corresponding downlink frequencies are obtained [11]. During analysis part, ARFCN from 26 to 37 were captured on Wireshark terminal. These are indicated in Table I.

For P-GSM (900) band:

$$F_{\text{downlink}}(n) = [45 + (890 + 0.2n)]\text{MHz} \quad (1)$$

Where n lies from 1 to 124.

The Discrete Fourier transform of active channels present in a given area is displayed on GNU Radio. In Wireshark, an interim buffer is created that can hold the known burst. The burst is then forwarded to the socket identified in Wireshark

TABLE I: Scanning GSM 900 Band

Absolute Radio Frequency Channel Number(ARFCN)	Channel Frequency
26	940.2 MHz
27	940.4 MHz
28	940.6 MHz
29	940.8 MHz
30	941.0 MHz
31	941.2 MHz
32	941.4 MHz
33	941.6 MHz
34	941.8 MHz
35	942.0 MHz
36	942.2 MHz
37	942.4 MHz

as 127.0.0.1:4729 on loopback(lo) which entitles the port GSMTAP [12]. Despite the fact that packets are discarded after being received by the destination, it can still be captured using Wireshark on port 4729 with loopback(lo) by the help of capture filter provided the downlink is still running. Consequently, Wireshark provides a complete software front end user interface to the GSM protocol analyzer due to its capability in dissecting GSM frames.

V. Results

With the discussion done above, P-GSM traffic was captured and analysed to verify the elaborated GSM protocol analyser with real world framework. The packets received at Wireshark terminal were only intended to get broadcast messages and signalling information. Hence, no infringement was established on GSM subscribers security and privacy.

The contents of the Broadcast Control Channel (BCCH) channel are generated at the BSC and are transmitted over the air as Radio Resource (RR) messages. A number of system information messages are defined to carry a plethora of system information parameters necessary for the MS, which includes system Information (SI) 1, 2, 3, 4 and 13. Apart from these, some other SIs (5 and 6) are transmitted on Slow Associated Control Channel (SACCH) to those MS which have active RR connection.

The contents of the SI are so distributed that the crucial information occur quite frequently. One particular example is of Random Access Channel (RACH) control parameter that comes in almost every SI resulting in a frequency of 4 times every second.

System Information Type 2 message as shown in Fig. 6 give the neighbouring cell channel description. The neighbouring cell description gives list of ARFCN which are meant for monitoring the BCCH of the neighbouring cells. Bitmap 0 indicates GSM 900 band being used, while variable bitmap shows GSM 1800 or 1900 being used. BA-IND is a BCCH allocation sequence number indication. It switches from 1 to 0 or vice -versa whenever the ARFCN of the user changes.

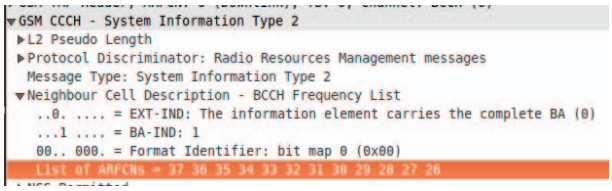

Fig. 6: System Information Type 2

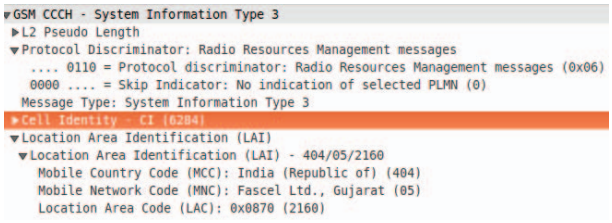

Fig. 7: System Information Type 3

System Information Type 3 message as shown in Fig. 7 give location area identification. The globally unique cell global identity (CGI) is formed by using a concatenation of the cell identity (CI) and location area identity (LAI). The LAI is broadcasted over the BCCH in different SIs. Along with the CI, LAI is also broadcast over SI 3. The LAI comprises of Mobile Country Code (MCC), Mobile Network Code (MNC) and Location Area Code (LAC).

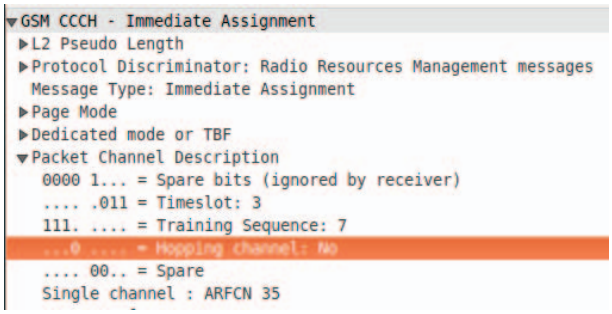

Fig. 8: Immediate Assignment with no hopping channel

The Mobile Country Code (MCC) is of 3 digits followed by the Mobile Network Code (MNC) of 2-3 digits and lastly the Location Area Code (LAC) represented by 2 octets, i.e. 0-65535 for different LACs . Cell Identity (CI) of two octets (16 bits) identifies a cell within a location area. The CI 6284 captured by Wireshark is identical with the CI of the designated test phone device used.

The MS can initiate the establishment of the Radio Resource (RR) connection by sending a channel request message over RACH. The BSC, in turn, assigns resources for the RR connection by sending an immediate assignment command to the MS over Access Grant Channel (AGCH). Immediate assignment message as shown in Fig. 8 give packet channel description of the obtained ARFCN. It consists of hopping channel data, time slot number and training sequence.

The channel description facilitates frequency hopping by

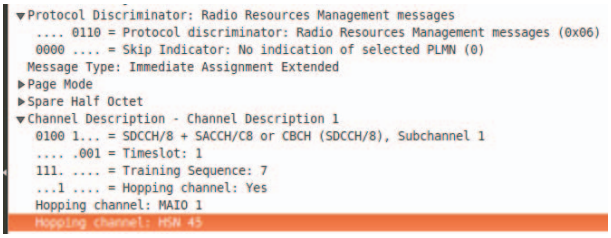

Fig. 9: Immediate Assignment with hopping channel

providing a list of freqeuncies that are used to decode the mobile allocation. The mobile allocation provides a list of RF channels belonging to the cell location (coded with binary '1' in the channel description as shown in Fig. 9), which is used in the mobile hopping sequence. All dedicated channel types and their associated channel types can hop. However, frequency hopping of BCCH channel is not permitted. When hopping channel is present, the immediate assignment message gives the information regarding hopping parameters such as the Mobile Allocation Index Offset (MAIO) and the Hopping Sequence Number (HSN) as shown in Fig. 9. The HSN 45 obtained in Wireshark is identical with the HSN of the designated test phone device.

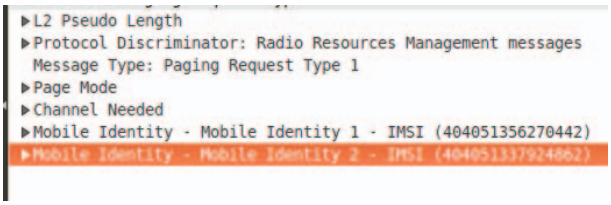

Fig. 10: Paging Request Type 1

The Paging Channel (PCH) and Access Grant Channel (AGCH) are collectively known as downlink Common Control Channels (CCCH). The PCH is used for paging wherein the MS is informed about an incoming call or sms. The MSC/VLR sends a paging message to one or more BSC and the BSCs, in turn, send the RR paging command to the MS. The paging messages can be grouped depending upon the number of MS that are paged and whether TMSI/IMSI are used for paging. For this purpose, three types of paging messages are defined in the Radio Resource (RR) management, i.e paging type 1, paging type 2 and paging type 3. Paging request types 1, 2 and 3 on wireshark contains MS identity which can be a temporary identity called Temporary Mobile Subscriber Identity (TMSI) or a permanent identity (IMSI) as shown in Fig. 10.

VI. Future Scope

Despite the fact that Airprobe can handle full-rate traffic channel decoding, there is still a lot of research improvement required in handling half-rate channels. The other area which needs attention is the enhancement of security in hopping channels by upgrading the current encryption algorithms. This can be established by thorough analysis and recommendations on currently available GSM data and its security.

VII. Conclusion

RTL-SDR is a cost-effective hardware, with compatible flow graphs for USRP. This is of extreme importance since GSM Technology is constantly going forward from year to year. The publicly available specifications of GSM are verified to comply with the extremely closed GSM industry. With some affordable tools like GNU Radio and Wireshark available, practical research of the GSM industry has become viable. This gives subscribers the ability to verify the workings of GSM, e.g. to check whether, and what kind of, encryption is being used to protect their conversations. The key feature of GSM is on-the-air-privacy. During this project, it was verified that observed cell towers used both frequency hopping and encryption. Airprobe limits itself to the downlink side of the air interface - cell tower to mobile phone. The bandwidth for specific network providers was reckoned during the project, along with the IMSI number, ARFCN channel in use and the Location Area Identification (LAI) of the mobile device of the respective network. The captured cell ID too was verified from the designated test phone device.

References

[1] A. Mehrotra and L. S. Golding, "Mobility and security management in the gsm system and some proposed future improvements," *Proceedings of the IEEE*, vol. 86, no. 7, pp. 1480–1497, 1998.

[2] F. Hillebrand, *GSM and UMTS: the creation of global mobile communication*. John Wiley & Sons, Inc., 2002.

[3] S. M. Siddique and M. Amir, "Gsm security issues and challenges," 2006.

[4] K. Vachhani and R. A. Mallari, "Experimental study on wide band fm receiver using gnuradio and rtl-sdr," in *Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on*. IEEE, 2015, pp. 1810–1814.

[5] G. Gu and G. Peng, "The survey of gsm wireless communication system," in *Computer and Information Application (ICCIA), 2010 International Conference on*. IEEE, 2010, pp. 121–124.

[6] A. Mehrotra, *GSM system engineering*. Artech House, Inc., 1997.

[7] K. Vachhani, "Multiresolution analysis: An unified approach using discrete wavelet transform on gnu radio," in *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on*. IEEE, 2015, pp. 887–892.

[8] M. Ettus, "Usrp user?s and developer?s guide," *Ettus Research LLC*, 2005.

[9] M. Sruthi, M. Abirami, A. Manikkoth, R. Gandhiraj, and K. Soman, "Low cost digital transceiver design for software defined radio using rtl-sdr," in *Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on*. IEEE, 2013, pp. 852–855.

[10] U. Lamping, R. Sharpe, and E. Warnicke, *Wireshark User?s Guide For Wireshark 2.1*, 1st ed., 2016. [Online]. Available: https://www.wireshark.org/download/docs/user-guide-a4.pdf

[11] M. Hadzialic, M. Skrbic, K. Huseinovic, I. Kocan, J. Musovic, A. Hebibovic, and L. Kasumagic, "An approach to analyze security of gsm network," in *Telecommunications Forum Telfor (TELFOR), 2014 22nd*. IEEE, 2014, pp. 99–102.

[12] S. Aragon, F. Kuhlmann, and T. Villa, "Sdr-based network impersonation attack in gsm-compatible networks," in *Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st*. IEEE, 2015, pp. 1–5.