Evaluation of 4G-LTE security and realization of a test stand for redirection attack

Michał Gronau
Department of Radio Communication Systems and Networks
Gdańsk University of Technology
Gdańsk, Poland
line 5: email address or ORCID

Arkadiusz Bysewski
Department of Radio Communication Systems and Networks
Gdańsk University of Technology
Gdańsk, Poland
line 5: email address or ORCID

Jakub Filipiak
Department of Radio Communication Systems and Networks
Gdańsk University of Technology
Gdańsk, Poland
line 5: email address or ORCID

Kamil Kobierzyński
Department of Radio Communication Systems and Networks
Gdańsk University of Technology
Gdańsk, Poland
line 5: email address or ORCID

Adam Trzebiatowski
Multimedia Systems Department
Gdańsk University of Technology
Gdańsk, Poland
line 5: email address or ORCID

***Abstract* — LTE (Long Term Evolution) is the most popular mobile communication standard worldwide [1]. It coexists with older: 2G, 3G and newer: 5G generations of mobile network standards. The coexistence with older generations poses severe threats to the security of the whole system. In this paper the team answers the question if it is possible to disrupt 4G-LTE transmission using dedicated tools. The team examines 3 possible attacks and performs them using SDR (Software Defined Radio) devices. The redirection attack is the most significant one as it enables the potential attacker to proceed with serious crimes. After the in-depth description of each attack the team presents the current state of GSM (Global System for Mobile Communications) network in selected countries, possible countermeasures to these attacks and discusses results with potential solutions for network operators and mobile phones manufacturers.**

Keywords — LTE, LTE security, cybersecurity, attacks, LTE redirection, IMSI catcher, GSM, security solutions.

I. INTRODUCTION

LTE is a wireless data transmission standard that allows to achieve high transmission speeds – many times greater than any previous standards. In addition, its significant advantage is low transmission delays. This allows to increase the efficiency of the 4G network, as well as the possibility of running advanced applications – in addition to standard services, such as calls, SMS (Short Message Service) messages and access to the Internet. LTE standard has been very popular for several years now – access points are common in most urbanized places in the world, providing the basis for mobile Internet in today's form. Currently in Poland, the access to the LTE network has (in terms of coverage) about 97% of the population [2]. This is particularly important due to the wide range of devices compatible with the standard – practically every smartphone manufactured today can connect to the LTE network, and thus provide services such as web browsing, video streaming or online gaming almost in real time. In addition, the LTE network can be used by such devices as laptops and tablets, as well as by devices operating under the IoT (Internet of Things) concept. Over the past few years not only the number of devices, but also the average amount of data used for mobile transmission around the world has been gradually increasing. Current expectations indicate that the growth will be even faster [1]. Therefore, it is important to meet the needs of users and develop the network. An important feature of LTE standard is its coexistence with other mobile networks. This phenomenon is known as convergence. It means that LTE can operate in the same area alongside older generations – 2G and 3G. The physical layer in LTE is different from that of 2G or 3G. Currently work is underway to introduce the next generation network – 5G, which will also be able to coexist alongside LTE as its successor. An important aspect of LTE is to assure a security of data transmission. The standard is described as secure, especially in comparison with 2G and 1G networks, but it is still vulnerable to implementation flaws in the protocols allowing e.g. location leaks. Moreover, a threat can be posed by hostile base stations that are not official access points of the operators to which the end devices can connect. The probability of such situation is minimized by using authentication numbers such as IMSI (International Mobile Subscriber Identity), TMSI (Temporary Mobile Subscriber Identifier), GUTI (Globally Unique Temporary Identifier) or IMEI (International Mobile Equipment Identifier). The architecture related to the network security includes such elements as NAS (Network Access Security) which ensures secure access to services via user authentication, encryption algorithms and device identification, NDS (Network Domain Security) which ensures secure signalling in the network and protects against wired attacks, UDS (User Domain Security) which is responsible for secure access to MS (Mobile Station) or ADS (Application Domain Security) which contains mechanisms ensuring secure transmission of messages between devices. However, part of the messages sent over the network to the terminal is sent without any authentication or encryption which is a significant disadvantage in the context of LTE security. In addition mobile technology standards, operating systems, hardware and network operations may be reasons for potentially weakened security.

II. LTE SECURITY ASSURANCE

In recent years, there has been a growing trend of cybercrime on the Internet. This is caused, among many things, by the rapid increase in popularity of devices that use network services, which increasingly being oriented towards user-friendly interfaces downplay the issue of security. In addition, weaknesses and vulnerabilities in communication protocols and almost unlimited number of guides showing how to properly carry out an attack make it necessary to implement increasingly precise defence systems, which also applies to mobile phone standards, including LTE. To fully understand how transmitted data is protected against

unauthorized access in LTE networks, it is necessary to familiarize with the network architecture, which is divided into 2 main parts: E-UTRAN (Evolved UMTS Radio Access Network) and EPC (Evolved Packet Core).

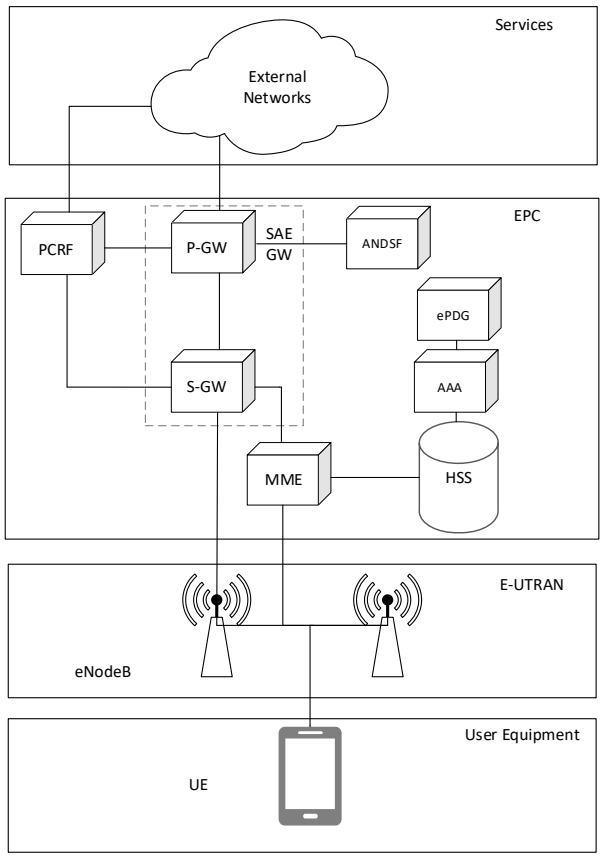

Fig. 1 Architecture of LTE network *[3] [4]*.

The first one contains eNodeB (Evolved Node B) elements that act as base stations and UE (User Equipment) elements which represent devices used directly for communication by the user [5]. The second part consists of 7 network elements. The first one is the MME (Mobility Management Entity), which is responsible for managing mobile communication sessions in the LTE network, performing the functions of subscriber authentication, network switching and call forwarding to other networks [6]. S-GW (Serving Gateway) is used to transport IP data traffic between UEs and external networks. P-GW (Packet Data Network Gateway) is a network node that connects the EPC to external IP networks and routes packets to and from these networks. In addition, it also assigns IP addresses to all UEs and enforces various policies on IP user traffic such as packet filtering. HSS (Home Subscriber Server) is a database that stores users' IDs and encryption keys [7] [8]. ANDSF (Access Network Discovery and Selection Function) is responsible for access network discovery and selection and ePGD (Evolved Packet Data Gateway) is responsible for the interaction between the EPC and untrusted non-3GPP networks that require secure access, such as Wi-Fi, LTE metrocells and femtocells access networks. Such an extensive architecture which provides access to a rich set of services needs robust security for sensitive user data and information sent during the LTE transmission.

One factor that makes the LTE network more secure than its predecessors is the way how the connection procedure is realized.

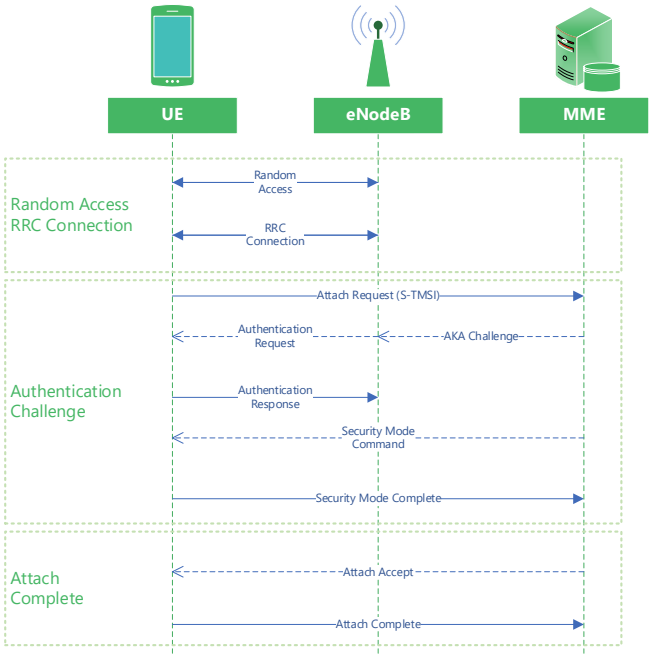

Fig. 2 Connection procedure in the LTE network *[9]*.

The UE sends the first "Random Access" message to the discovered eNodeB that has the highest power and is eligible for attempting the connection procedure. This is necessary to allow the end device's clock to synchronize with the network's clock and to assign it a dedicated channel to receive messages. As a result, it is possible to run RRC (Radio Resource Control) protocol allowing the implementation of resource management strategies. After basic information is exchanged between the mobile device and the base station, the "Authentication Challenge" procedure is initiated to ensure proper security during a call or data transmission. To execute it correctly, it is necessary for the UE to be identified. The MME needs to know which user wants to exchange information. It is possible to distinguish each user by unique IMSI number assigned to the SIM (Subscriber Identity Module) card. To protect the privacy of the user, its transmission over the radio network is limited to minimum. Instead, a temporary GUTI number assigned to the user by the MME is used. GUTI consists of GUMMEI (Globally Unique Mobility Management Entity Identifier), which uniquely identifies the MME and M-TMSI (Mobile Temporary Mobile Subscriber Identity) which identifies the user. An abbreviated version of GUTI is sent during "Attach Request" message as S-TMSI. It contains the identity assigned to the user by MME and is used to call the user [10]. Another security procedure that makes a MITM (man-in-the-middle) attack almost impossible is the AKA (Authentication and Key Agreement) encryption. This is a protocol used by the EPC for proper verification of a mobile device. It enables a two-step authentication procedure whereby the mobile terminal as well as the network authenticate each other in order to check whether they are indeed the devices they claim to be. This is done by generating sets of encryption keys by each device involved in the communication. Combined with mechanisms that protect the keys from premature obsolescence the result is, in theory, a highly secure network in which the keys are

known only locally by devices communicating with each other. If authentication passes, the eNodeB sends a Security Mode Command message to the UE protected by the integrity principle. The UE enters data that is associated with integrity protection algorithm indicated in Security Mode Command, and then verifies integrity of received Security Mode Command by checking the MAC (Message Authentication Code). If Security Mode Command message does not pass the integrity protection check, UE will send a Security Mode Failure to the eNodeB – the connection will not be established. If on the other hand the integrity protection check passes, UE will insert the encryption keys KRCenc and KUPenc associated with the encryption algorithm indicated in the Security Mode Command. From then on, encryption will be applied to all subsequent messages received and sent by UE, except for Security Mode Complete message, which is not encrypted [11]. Another reason why LTE is a standard with maintained high security is the use of USIM (Universal Subscriber Identity Module) cards, the successors to SIM (Subscriber Identity Module) cards, which enable mutual authentication. USIM card use longer encryption keys and also allow creating a list of networks inaccessible to the device. Moreover, an important fact from a security perspective is that a USIM cards store the subscribers' IDs – their unique identifiers.

III. Security threats of the LTE network

Having all the security mechanisms in LTE does not mean it is completely secure. There are many elements that are used for attacks carried out in these networks. First of all, there are fake base stations and fake terminal devices. Moreover, IMSI identification number, MIB (Master Information Block) and SIB (System Information Block) messages can be used to conduct attacks. IMSI number is assigned uniquely to each user and because it is an extremely sensitive data, it should be inaccessible to third parties. To make it less vulnerable to leaks, it is being hidden using TMSI and GUTI identifiers. Unfortunately when UE is being connected for the first time IMSI is sent as a plain text and not encrypted in any way [12]. MIB and SIB broadcast messages are present in an unencrypted form during the synchronization of terminal devices with the base stations and they are sent almost continuously.

Attacks on LTE networks can be divided into passive and active attacks. The passive ones get their name from the fact that they do not make any changes to the transmitted data, which makes them practically undetectable. Their goal is to track and intercept data of a victim in order to gain as much information as possible. An example of such attack can be sniffing. It consists of listening to the network traffic and collecting all the necessary data to be able to properly perform an active attack. An active attack differs from a passive one as it creates or modifies the transmitted data stream in order to achieve goals intended by the attacker [13]. This type of attack can include DoS (Denial-of-Service) attacks that prevent users from accessing selected services forcing a downgrade from LTE to 3G or even 2G or creating a fake base station based on information obtained during the passive attack. Attacks can be divided also in another way – basing on the network element that will be attacked. One of them is attack on RAN (Radio Access Network). Weaknesses present in this part of the network make it possible to sniff broadcast channel information, retrieve IMSI, reveal the location of an LTE device or jam communications. DoS attacks mentioned earlier also occur in this part of the network as well as forcing the downgrade to 3G and 2G standards. The second type of attack is an attack on the core network. This type of attack is very dangerous from the point of view of mobile network operator, because it covers more than one or a group of users. In this part of the network there are APT (Advanced Persistent Threat) attacks which are motivated by political or economic motives. They aim at stealing data, spying or causing large financial losses to the attacked company. Additionally, DoS attacks launched in this part of the network have much greater consequences as they affect many network users. Attacks of this type can be implemented using a botnet or saturation of HSS database or S-GW gateway [14] [15].

Next type of attack that is carried out against LTE network is a MITM attack. It consists of sniffing and modifying messages sent between two parties without their knowledge and makes it possible to extract a lot of sensitive user data. An example of such attack can be handing over the sender's own key during a transmission protected by asymmetric cipher. To perform a MITM attack, it is necessary to create a malicious base station that has to imitate real network operator's one and force the UE to connect to it [16]. In order for the end device to successfully connect to the malicious base station, it is necessary for the fake base station to have set the highest Absolute Priority, Radio Link Quality and Cell Accessibility in order to have higher transmission power than the real base station. Considering the parameters of the fake base station – they have to be identical to the original base station to enable imitation. Proceeding the last condition is possible by using a passive type of sniffing attack. It is necessary to intercept MIB, SIB1 and SIB5 messages. From the first two messages it is crucial to extract the following information: PLMN identity (Public Land Mobile Network identity), Downlink-Bandwidth and TAC (Tracking Area Code). If one wants UE to start the connection procedure, the fake base station has to provide the same values of these parameters as the real base station. Using SIB5 message it is necessary to retrieve, among other data, information such as Downlink-Carrier-Frequency and cellReselectionPriority. In order for the attack to be successful, the latter value has to be set to the highest possible: 7. As a result, end devices in the closest proximity will connect to the fake base station. Since the temporary GUTI identifiers are unknown, "new" UEs are forced to introduce themselves using their unique IMSI numbers. In this way, the first sensitive user data can be acquired [9].

Another attack that can be carried out is forcing a downgrade from LTE network to the older generation network – 3G or 2G [17]. In this case, vital information such as security keys are sent without encryption and it is possible to sniff conversations and view text messages, and most importantly, perform a MITM attack. The switchover to legacy networks is possible, because LTE standard does not have mutual authentication and encryption at the initial connection stage, allowing UE to accept "reject" messages. In this case, end device sends a TAU (Tracking Area Update) Request message to the fake base station even though it is connected to the real base station all the time. TAU Request message is integrity protected but not encrypted (NAS security), so it is easy to decode this message [18] and send "TAU Reject" message with set value "EMM cause number 7: LTE services not allowed". In this situation the UE deactivates all services related to the real network and to regain lost services it can try to connect to 2G or 3G network.

If 2G or 3G connection is made, it means that the attack has succeeded and it allows to proceed with even more attacks.

IV. Hardware and software solutions used for the attacks

In case of proceeded attacks open source software was used. There is a lot of software available on the Internet allowing to set up local 2G/3G/4G/5G networks. These networks can be run using SDRs, such as USRP B200mini. SDR is a device that acts as a radio frontend for PC software and allows to receive and send various radio signals. The team planned to use Osmocom environment and srsLTE software, however as a consequence of relatively high complexity of srsLTE source code, OpenLTE solution was chosen instead. These software solutions can be described as follows:

A. *OpenLTE* – it is an open source implementation of the 3GPP LTE specifications. The focus is on transmission and reception of the downlink *[19]*. It is developed by a single developer. The source code is very well organised and its structure is well-rounded. It is easy to modify, recompile and reinstall the source code. It allows to run LTE eNodeB with all required modules allowing to proceed any desired attacks.

B. *Osmocom* – the Osmocom project is an umbrella project regarding Open source mobile communications. This includes software and tools implementing a variety of mobile communication standards, including GSM, DECT (Digital Enhanced Cordless Telephony), TETRA (TErrestrial Trunked Radio) and others *[20]*. The GSM part consists of many subprograms: OsmoHLR, OsmoMSC, OsmoMGW, OsmoSTP, OsmoBSC, etc. Each of them can be configured individually via Telnet and a config file, which allows for some extra flexibility running this software.

C. *OsmocomBB* – OsmocomBB is an Open Source GSM Baseband software implementation. It intends to completely replace the need for a proprietary GSM baseband software, such as drivers for the GSM analog and digital baseband or the GSM phone-side protocol stack, from layer 1 up to layer 3. OsmocomBB allows to use a compatible phone, e.g. Motorola C139, as a working platform for modified mobile phone software *[21]*.

In case of the project, mainly USRP B200mini devices were used. The USRP B200mini delivers a 1x1 SDR/cognitive radio in the size of a business card. With a wide frequency range from 70 MHz to 6 GHz and bandwidth up to 56 MHz [22], it is an ideal solution for running local mobile networks base stations and access points or UEs. USRP devices work with UHD (USRP Hardware Driver) library making them compatible with a wide range of SDR software (including e.g. GNU Radio).

For running OsmocomBB based mobile phone code the team used unmodified Motorola C139 phone with USB to RS-232 (TTL) converter and custom 2.5 mm audio jack plug.

Base stations and access points software pieces were running on PCs with a Linux-based operating systems (64-bit Ubuntu) installed.

Depending on the location of conducting the experiments, 2 different spectrum analysers were used: Anritsu MS2721B spectrum analyser with OA2-0.3-10.0V/1505 omnidirectional antenna and Narda SRM-3006 spectrum analyser with Narda 3502/01 isotropic antenna.

The 2 used PCs are laptops equipped with AMD Ryzen 3200U and AMD Ryzen 4800H CPUs (Central Processing Units) respectively. They have 16 GB of RAM (Random-Access Memory). Their specifications are well beyond the minimum requirements of OpenLTE and Osmocom software, however it was important for them to support USB 3.1 Gen 1 connectivity, as USRP B200mini requires it to work properly [22].

The victims' UEs were selected mobile phones as follows: Samsung Galaxy S6 (Android 7.0), Samsung Galaxy S7 (Android 8.0.0), Xiaomi Mi 10 Lite 5G (Android 11) and Xiaomi Mi A2 Lite (Android 9).

For analysing local mobile networks presence (2G and 4G) the team used the following applications: RSSI from Osmocom [23], Network Cell Info Lite [24] and LTE Discovery [25].

The team planned to perform all the attacks in a simulated environment. Unfortunately due to COVID-19 restrictions, the team had to conduct all experiments remotely. With a limited number of SDRs available, instead of a simulation, a series of controlled attacks in closed controlled environment was carried out. Extra safety measures were ensured in order to guarantee that no nearby UEs were affected by these experiments. Moreover, the electromagnetic spectrum was constantly monitored with a high quality spectrum analyser.

V. First proposed attack: a phone number catcher (including MITM method)

At first our team proceeded with MITM attack, including a downgrade from LTE to 2G [12]. This attack allows to catch victim's MSISDN (Mobile Station International Subscriber Directory Number) – a phone number.

A. The architechture of the attack

The general architecture of this attack from hardware perspective can be presented as in Fig. 3. It consists of 2 SDRs (B200mini), Motorola C139 phone, 2 PCs and a victim UE. The numbers visible next to the objects represent the approximate sequence. The victim UE has a commercial SIM card inserted and is working normally with a commercial LTE access point. The second PC which runs Osmocom software has to maintain OsmocomBB as well. That is because these 2 pieces of software have to communicate each other in order to successfully conduct a phone number catcher MITM attack.

In the Fig. 4 there is a software architecture of the attack. All the general requirements and assumptions from the software perspective are present. One of the main advantages of presented architecture is the fact that it is not a typical RF (Radio Frequency) jamming. This kind of attack does not require a significant transceiver power. The rogue eNodeB is set to use signalling messages to redirect the victim UE to the local rogue GSM BTS (Base Transceiver Station). It means other commercial networks do not have to be jammed (e.g. 3G) because the signalling messages will point at a desired 2G BTS.

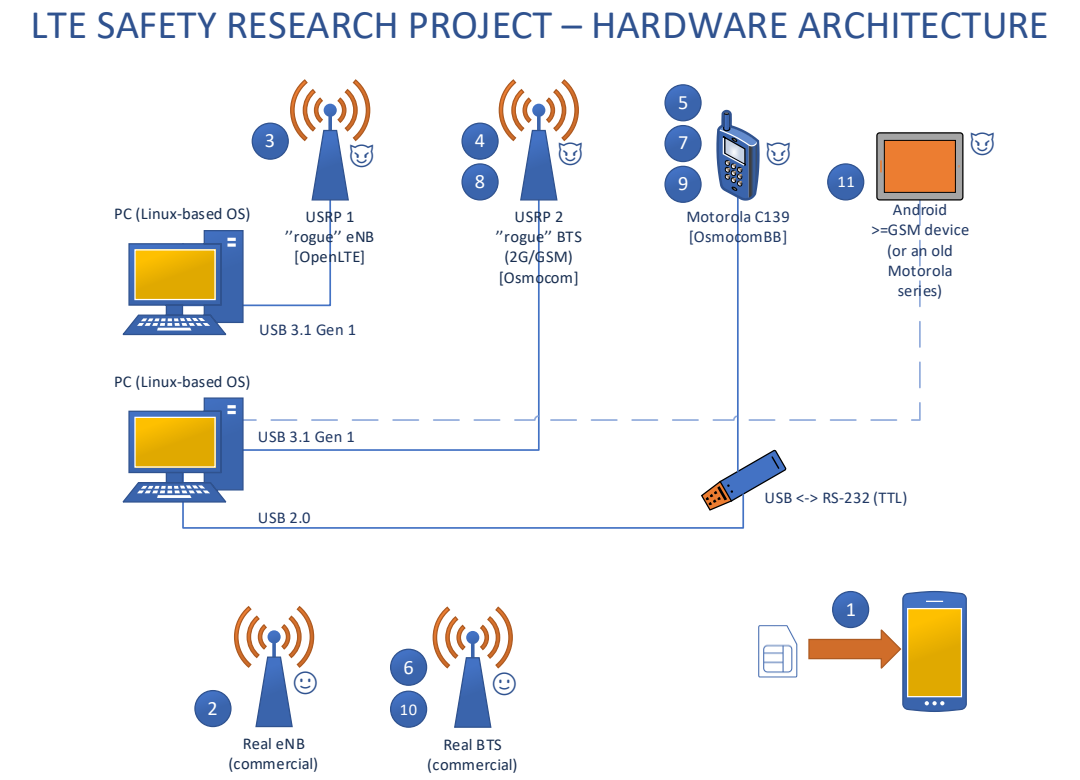

Fig. 3 Hardware architecture of phone number catcher attack

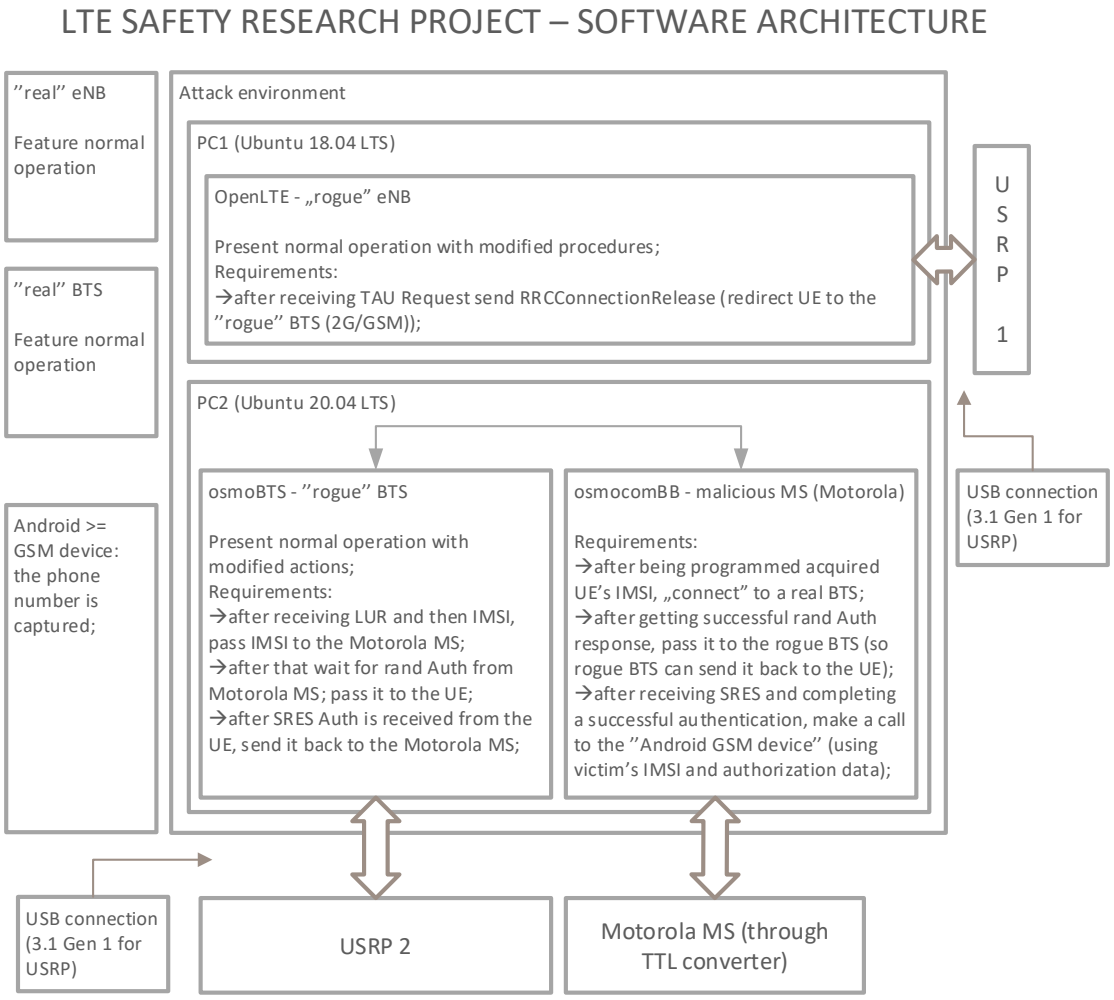

Fig. 4 Software architecture of phone number catcher attack

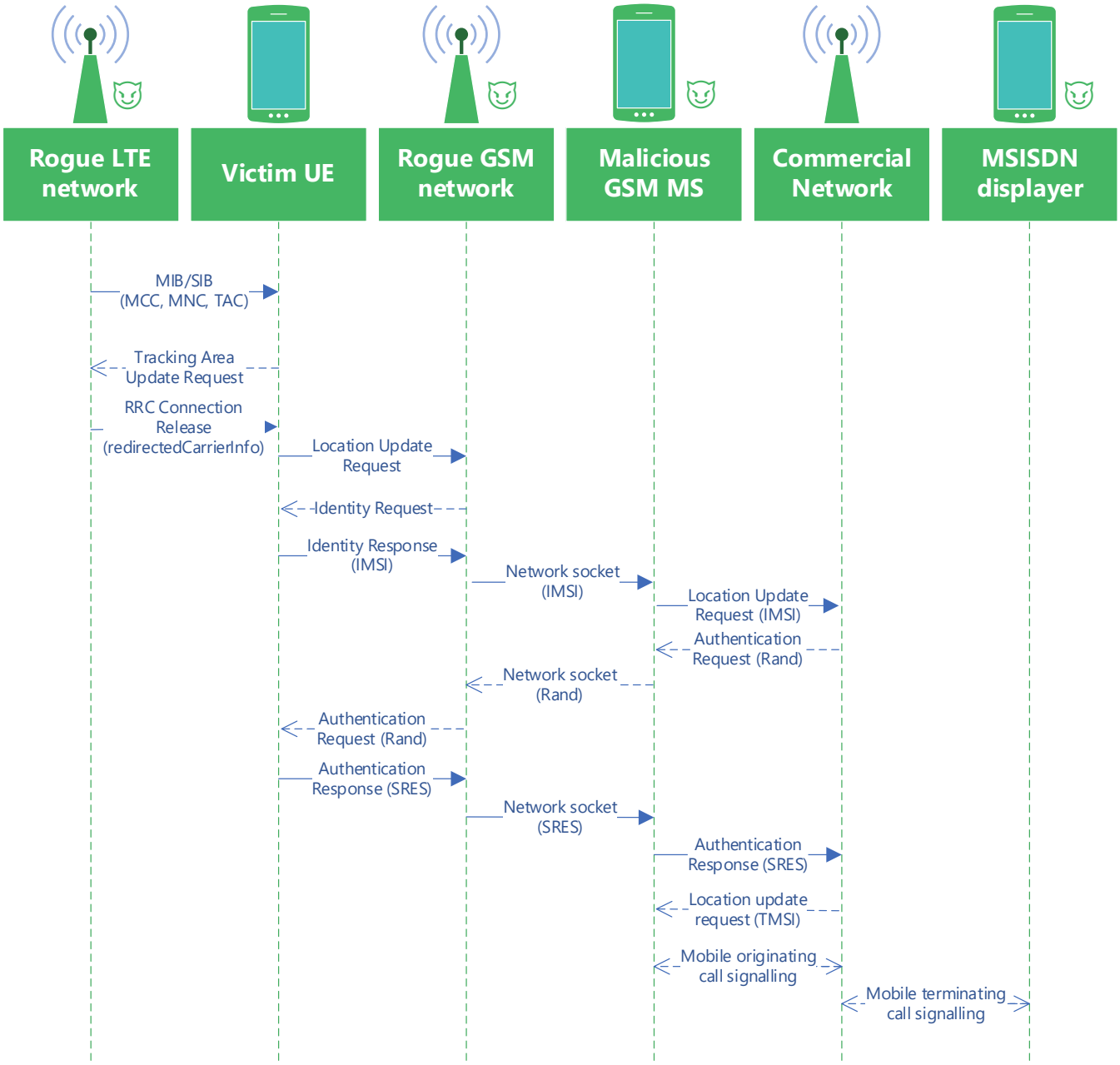

Fig. 5 Theoretical signalling process of LTE Phone number catcher attack

The goal of the first proceeded attack is to perform a redirection from the commercial LTE network to the rogue GSM BTS. The next step relies on OsmocomBB mobile phone software posing as a victim UE (using its IMSI number), logging in the commercial GSM network as a victim UE. After that it is possible to make a call to the attacker's phone. The commercial base station has the necessary information about the linkage between IMSI number of the victim UE and MSISDN number of the victim UE. Thanks to that the victim's phone number is displayed on the attacker's phone screen.

The signalling process is present in the Fig. 5. At first the rogue eNodeB sends the broadcast messages. EARFCN (E-UTRA Absolute Radio Frequency Channel Number) is the same number as used in the real LTE access point. Then the victim UE receives all the information about the rogue access point – MCC (Mobile Country Code), MNC (Mobile Network Code) and TAC. When the criteria for eNodeB reselection are met, the victim UE starts TAU procedure. Next the rogue eNodeB sends RRCConnectionRelease (RRC – Radio Resource Control) message back to the victim UE. This message makes it impossible for the victim UE to continue the procedure of connecting to the rogue eNodeB. Instead the RRCConnectionRelease message contains redirectedCarrierInfo information, which points at the new base station, to which the victim UE is forced to connect. The parameters included in redirectedCarrierInfo have to be exactly the same as the Osmocom BTS (Rogue GSM network) is configured. Then the signalling process is handed over to Osmocom software, as the victim UE tries to connect to it.

The victim UE sends LUR (Location Update Request) message to the local rogue GSM network. Osmocom receives

information that the UE requests a connection with it. Later on it sends Identity Request to the victim UE. Then the victim UE sends IMSI number back. Having the IMSI number it is possible to start the connection procedure for the malicious GSM MS (using victim's UE's IMSI). The IMSI number is sent from OsmoMSC to OsmocomBB via local network socket [26]. It allows OsmocomBB to use the spoofed IMSI number of the victim's UE. Then OsmocomBB sends LUR message to the commercial GSM network in order to connect to it. The commercial GSM network detects this request as a usual request, therefore it sends Rand number back to the OsmocomBB software, continuing the procedure of authentication. When OsmocomBB receives Rand number, it forwards the number to the OsmoMSC. Thanks to this OsmoMSC can send it back to the victim UE, continuing the procedure of authentication. Then the victim UE generates SRES (Signed Response) number, which is based on Rand number and Ki (Subscriber key) saved in the SIM card. The SRES number is also generated at the commercial base station. The GSM base station is basing on the same input parameters to generate it. If the commercial GSM network receives the SRES number and it equals to the locally generated SRES number, that means the process of authentication is complete and the LUR procedure ends with LUA (Location Update Accept) message. In case of the analysed attack OsmocomBB should receive TMSI number. It means it can now send SMS messages and make phone calls as a normal UE (using victim's UE's identity). After that the attack is complete [12].

B. The implementation of the attack and the results

The team has successfully implemented all the signalling process relying on a network socket marked in the orange frame visible in the Fig. 6.

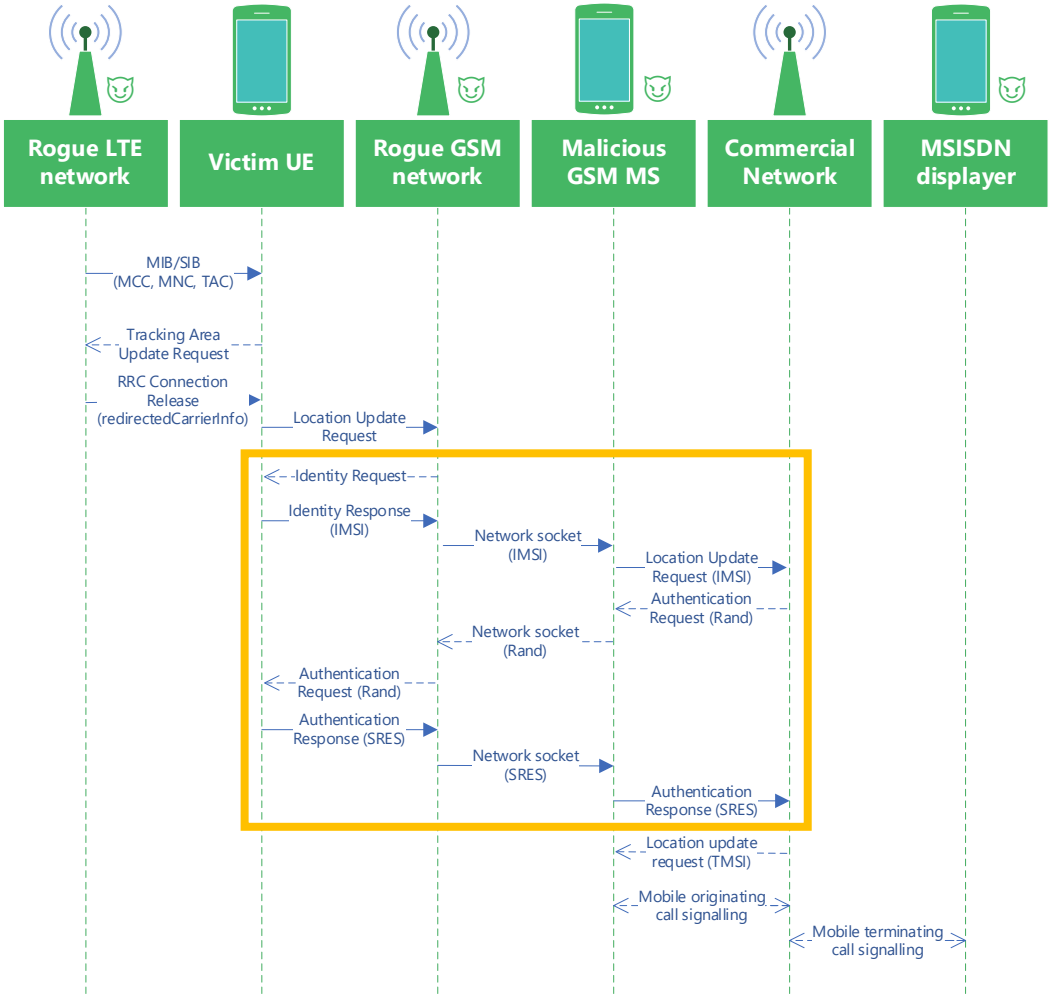

Fig. 6 Implemented signalling process of LTE Phone number catcher attack

All the signalling process has been thoroughly tested and validated. It worked properly, however no authentication completion was observed. This is due to fact that Polish telecommunication operators accept A5/1 ciphering algorithm exclusively. Forcing A5/0 (no ciphering) or A5/3 (stronger ciphering) does not result in proper MS authentication ("Location update failed" message present in OsmocomBB log).

The presence of obligatory A5/1 ciphering is the reason why despite implemented signalling the authentication process does not end successfully. At the bottom of the orange frame (Fig. 6) there is the SRES message forwarded to OsmocomBB (malicious GSM MS). After the SRES message is sent to the commercial GSM network, the network immediately starts ciphering all the messages using A5/1 algorithm. A5/1 algorithm uses Kc (Ciphering key), which is based on Rand number and Ki key. All the subsequent messages are encrypted which means OsmocomBB cannot

decode them properly. All the signalling process is progressing as planned, however the malicious MS is not able to communicate with the commercial GSM BTS because the Kc key is unknown. It is a significant obstacle which makes MITM phone number catcher attack impossible to perform without making further modifications, namely extracting Kc session key using Kraken algorithm leveraging rainbow tables [27]. After acquiring Kc key it is possible to encrypt and decrypt all transmitted messages, therefore a call request may be carried out. The team decided not to continue with Kraken decryption algorithm hence this attack cannot be performed.

It is worth noting that there were successful attempts to perform a MITM attack as shown in [28].

VI. Second Proposed Attack: Rogue Foreign GSM BTS with a Foreign SIM Card

The team conducted a second experiment as a possible attack which involved foreign SIM card (namely Czech SIM card from Czech telecommunication operator – OpenCall).

A. *The architecture of the attack*

The attack is not complex in its structure. It is based on a properly configured Osmocom environment which poses as a legitimate OpenCall base station. Naturally, in Poland there are no Czech base stations. The presence of rogue OpenCall GSM BTS creates a situation when the victim UE is going to connect to the rogue BTS because it is discovered as a home base station and it is going to be preferred over any roaming base stations or access points. It is necessary to configure OsmoHLR part in such a way that it would accept any subscribers without any authentication or encryption even if they are not present in HLR (Home Location Register) database.

B. *The implementation of the attack and the results*

During the experiment Samsung Galaxy S6 phone was used with OpenCall USIM card. Osmocom environment was configured to identify as a legitimate home O2 base station (OpenCall is MVNO – Mobile Virtual Network Operator – and it uses O2 operator base stations). The authentication and encryption mechanisms were deliberately disabled. When Osmocom environment was running, the victim UE (Samsung Galaxy S6) almost immediately connected to the rogue GSM BTS. It was happening repeatedly even though secure roaming networks: 2G, 3G and 4G were nearby available.

Fig. 7 Status icons on Samsung Galaxy S6 phone with Czech USIM card - no roaming icon present

The only real indicator for the victim that they are under attack is the presence of home base station in a place where it should not be present and a lack of "R" icon indicating active roaming status – as shown in Fig. 7. The result of the experiment is as follows: the UEs prefer to connect to the home base station at all costs. If any (even not secure) home BTS is available, it becomes automatically a network of choice. This is a dangerous behaviour of UEs and can be used against them. The real scenario for such attack is e.g. an airport where a lot of foreigners arrive. A skilled attacker would be able to eavesdrop on phone calls, read sent SMS messages or even extract sensitive data using e.g. fake DNS server associated with Osmocom EDGE (Enhanced Data rates for GSM Evolution) connectivity settings.

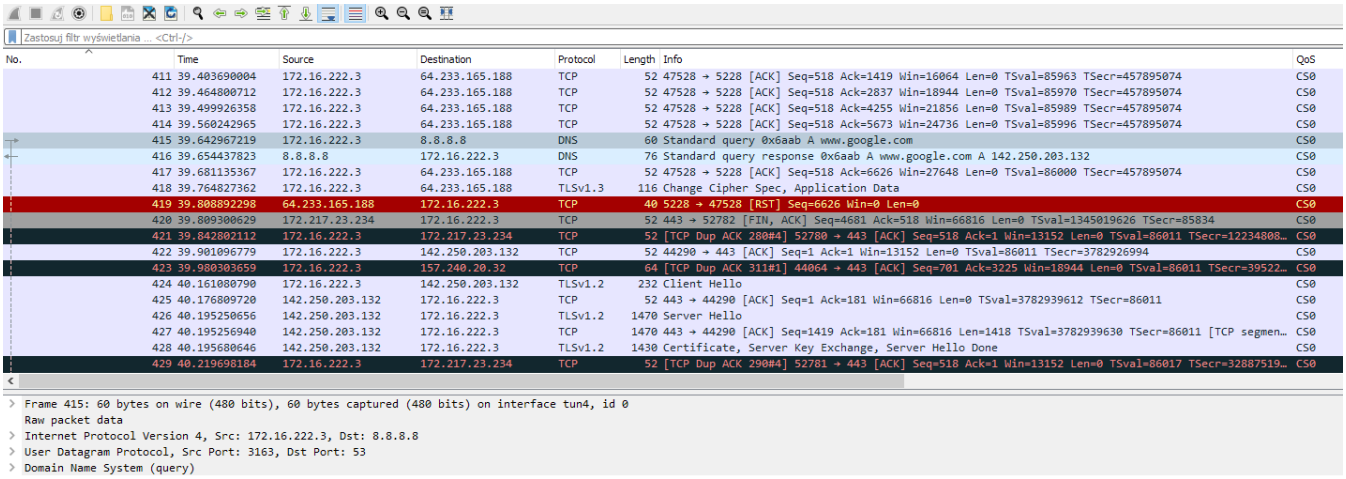

Fig. 8 Captured packets on a virtual tun4 interface - sniffing possibilities

VII. Third Proposed Attack: A Redirection Attack to the Insecure Rogue GSM Network

The third experiment was based on the first attack proposed. The LTE part was basically the same (redirection), however the GSM part was vastly different from what is presented in chapter V.

A. *The architecture of the attack*

The architecture is similar to that present in Fig. 5. The initial procedure which relates to the LTE signalling is exactly the same. It means the UE is at first redirected to a specific GSM BTS which in this case is Osmocom configured BTS. After LUR message is sent by the victim UE, the normal connection procedure takes place. An important part of the connection process is that Osmocom BTS is not secured in any way – authentication and encryption are deliberately disabled. The rogue GSM network accepts all subscribers, no matter if they exist in HLR database. After connection is established, the rest of the process looks very similar to the case presented in chapter VI.

B. The implementation of the attack and the results

For the first experiment made (chapter V) the team focused on GSM signalling exclusively. In order to properly conduct a redirection attack, the team made an additional research. As a result the team managed to acquire preprepared Ubuntu image containing necessary source codes and binaries for proceeding the redirection attack, made by Bastien Baranoff – an enthusiast in the field of mobile networks security [29]. After acquiring the image, all the necessary modifications were made, OpenLTE solution was recompiled, reinstalled and configured.

The final configuration was based on real BTS and eNodeB from Polish network operator – Play. 4 UEs (enumerated in chapter IV) were used for the experiments. All of them had Play USIM cards inserted. The team conducted 4 experiments in a row. During each of them all 4 UEs were monitored, as well as OpenLTE and Osmocom logs.

The first experiment in a row consisted in turning on the rogue eNodeB and GSM BTS while all the UEs were in a state "as is", meaning no settings changes were made prior to the experiment. The first devices to connect to the rogue GSM BTS were Samsung Galaxy S7 and Xiaomi Mi A2 Lite. Samsung Galaxy S6 connected a few minutes later. Xiaomi Mi 10 Lite 5G did not connect to the GSM BTS at all during the first experiment – the only observed event was a downgrade from LTE to 3G. However it did not connect to the rogue GSM BTS, another observation was made. The signal power indicator visible on the status bar saturated almost immediately after the OpenLTE and Osmocom software run. Then there was no connection to the Internet network for a few tens of seconds until the switchover to the legitimate 3G Node B happened. The icon "LTE↓↑" was visible however only the arrow up was active. It means that there was no downlink as the UE tried to connect to the rogue LTE network. It is worth noting that Samsung Galaxy S7 and Xiaomi Mi A2 Lite UEs had mobile data switched off during the experiment. It may had an impact on their faster network reselection to the rogue GSM BTS but that has not been confirmed. Turning off the rogue eNodeB did not cause immediate network reselection from the rogue GSM BTS to a legitimate LTE eNodeB for a few minutes. The experiment showed the severe consequences for the subscribers using 3 out of 4 UEs. When any UE is connected to the rogue GSM BTS, it cannot make or receive any phone calls. An attempt to proceed a phone call was never successful, the process was terminating automatically almost immediately, without any information or sound signal. An attempt of a phone call test was visible in Osmocom logs:

```
<000e> gsm_04_08.c:1575 SUBSCR(IMSI-26006XXXXXXX634:TMSI-0x3D516FF2:TMSInew-
0x4006A5B4) VLR: update for IMSI=26006XXXXXXX634 (MSISDN=)
<000e> gsm_04_08.c:1575 SUBSCR(IMSI-26006XXXXXXX634:TMSI-0x4006A5B4) VLR: update
for IMSI=26006XXXXXXX634 (MSISDN=)
<0001> gsm_04_08_cc.c:1887 trans(NULL NULL callref-0x0 tid-0) rx MNCC_SETUP_REQ for
unknown subscriber number '485XXXXXXXX'
```

Fig. 9 A fragment of Osmocom log (OsmoMSC)

The team also tried to send SMS messages while being connected to the rogue GSM BTS. There were no signs that the messages have not been sent however for the obvious reasons the messages did not reach their recipients. The messages got stuck in the Osmocom environment. Additionally, the team tried to make calls using UE connected to the legitimate network to the UEs being under attack. These calls attempts resulted in many different findings. One of them was call-progress tone typical for connection setup [30]. Another scenario was that a "The number you're trying to reach is busy." message was played. The message can be misleading for the caller as it is not accurate. Moreover when the attacked UEs did not receive any notifications about missed calls after reconnecting with a legitimate base station. During the attack the subscribers still have access to the Internet network via EDGE technology. The packets can be captured in the same way as described in chapter VI. The ability of capturing the packets gives significant possibilities to the attacker as described previously.

In the second experiment airplane mode had been activated on all UEs before the rogue eNodeB and GSM BTS were turned on. 4 out of 4 UEs connected almost immediately to the rogue GSM BTS through LTE redirection. The results are vastly similar to the first experiment and remain accurate. An additional test was made: first the rogue eNodeB was turned off (the rogue GSM BTS was still active). Then airplane mode was turned on and off (on all UEs) at once. After deactivating airplane mode 3 out of 4 UEs reconnected to the rogue GSM BTS even though they were able to connect to a legitimate eNodeB at that time. The UEs reconnected with the legitimate eNodeB a few minutes later.

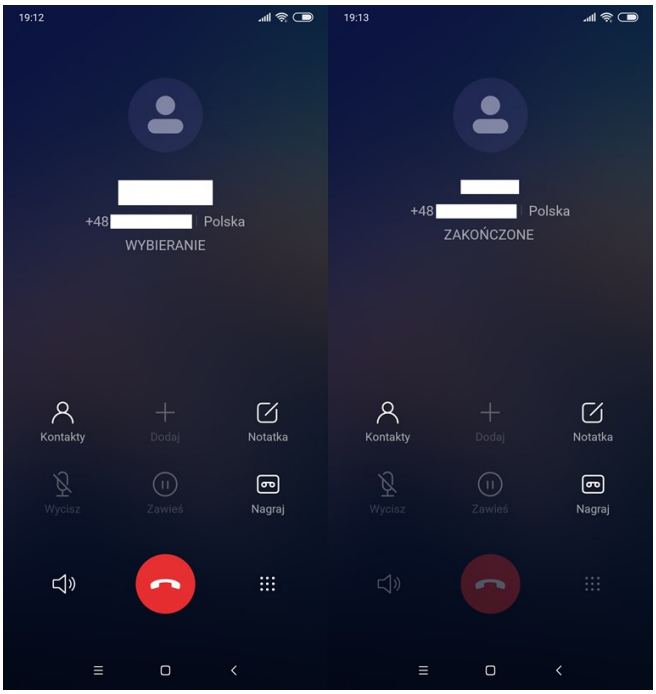

Fig. 10 An example of making a phone call from attacked UE Xiaomi Mi A2 Lite - a connection phase and immediate call termination

The third experiment was based on setting the mobile data option on and off on each UE. A certain relationship was observed, the UEs were connecting faster to the rogue GSM BTS when the mobile data option was switched off. This was not confirmed in the fourth experiment, therefore mobile data option may be irrelevant in case of legitimate eNodeB to rogue GSM BTS switchover timing. The timing may be related to some different parameters, e.g. T3412 timer expiration moment [31].

VIII. Results Commentary and Discussion

The hypothesis of the team's research is "It is possible to disrupt 4G-LTE transmission using dedicated tools" and it has been proved as confirmed as a final result. A set of open source software was run and a set of experiments was conducted. As shown in chapters V, VI and VII it is possible to perform various attacks related to LTE network. Especially the redirection attack was successfully proceeded from a legitimate LTE network to a rogue GSM BTS. The team's research shows that commercial mobile networks are prone to such attacks despite advanced security protocols present within LTE standard. It is clear that such attack may lead to a DoS for a group of users. Moreover, the downgrade to the rogue GSM network may occur. There are severe consequences to such a downgrade because 2G is especially prone to various attacks, such as MITM, number phone extraction, phone calls eavesdropping, SMS messages interception, etc. Importantly, the downgrade attack allows the subscriber to use EDGE services which may lead to Internet based attacks.

All these attacks can be proceeded with widely available SDRs which are relatively cheap [32]. In the project the team used a mid-range SDR – namely USRP B200mini. It is possible however to run srsLTE or OpenLTE software using a low-end SDR, such as LimeSDR starting at about $250 [33].

During the experiments the team observed that a downgrade to a rogue GSM BTS was not always the case. There were several situations when UEs reconnected to a legitimate 3G Node B. From a security perspective that is a better result however it does not dissipate the security concerns. The 3G network is set to be turned off in Poland in the next several years [34], while 2G network will continue its operation [35]. Some countries are actively quenching 3G networks, while some have already completely turned it off [36].

During the research the team analysed GSM encryption algorithms used in Poland. Currently the only accepted encryption algorithm is A5/1. A5/1 is one of the weaker variant which is prone to being cracked in a matter of minutes or even seconds [28]. The network operators could introduce more secure A5/3 encryption algorithm. This action however would require a reconfiguration of the whole 2G network and moreover a lot of compatibility issues would arise – not all GSM devices support A5/3 encryption algorithm. The best solution would be for the operators to completely shut down 2G network in favour of newer, more secure mobile network standards. Unfortunately this solution is not plausible due to significant GSM popularity [35].

In case of studied attacks manufacturers of UEs and operating systems for UEs have the greatest capabilities to prevent the attacks from happening. The team proposes a solution: in every phone's settings menu there should be an option allowing the user to completely disable the 2G connectivity. Moreover, the 2G connectivity should be disabled by default. If a user wanted to turn it on, they would have to be warned about possible negative consequences of using 2G network and its general insecurity. In that way the level of mobile network security would go up as a downgrade to GSM would be impossible. Unfortunately most of UEs do not allow the user to completely disable 2G connectivity. Some UEs allow to disable it by using a hidden testing menu (e.g. Xiaomi Mi 10 Lite 5G, using code *#*#4636#*#*). Xiaomi Mi A2 Lite allows the user to set many combinations of used mobile network standards directly in settings menu (xiaomi.eu firmware used):

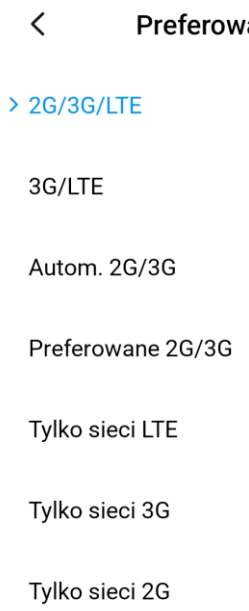

Fig. 11 A menu of network preferences, allowing the user to completely disable 2G connectivity

IX. Conclusions

The team has successfully conducted a series of experiments proving that it is possible to negatively influence the LTE transmission using widely available SDR devices. The hypothesis of this paper has been proved to be correct. The main goal which was to perform a phone number catcher attack was not fulfilled. Nevertheless a lot of important results have been observed and described how they compromise mobile network security. Example solutions have been presented in order to propose methods which would improve the mobile network security overall. Various actions can be taken both by mobile network operators as well as by phones manufacturers.

References

[1] Ericsson, „Ericsson Mobility Report," Ericsson, 2021.

[2] UKE - Office of Electronic Communications, „Report on the state of the telecommunications market in Poland in 2020," UKE, 2021.

[3] M. Kotuliak, „LTE Monitoring - Master Thesis," Department of Computer Science, ETH Zürich, Zürich, 2020.

[4] S. Gajewski, „Modern Radio Communication Systems," Gdańsk University of Technology, Gdańsk, 2020.

[5] K. Kohls, D. Rupprecht, T. Holz i C. Pöpper, „Lost traffic encryption: fingerprinting LTE/4G traffic on layer two," 12th ACM

Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19), 10.1145/3317549.3323416, 2019.

[6] M. Solutions, „Motorola Solutions - products," [Online]. Available: https://www.motorolasolutions.com/en_us/products/lte-broadband-systems/broadband-systems-equipment/mme.html#tabproductinfo. [Data uzyskania dostępu: 27 December 2021].

[7] IPLOOK, „IPLOOK - products," [Online]. Available: https://www.iplook.com/products/epc-sgw-pgw. [Data uzyskania dostępu: 27 December 2021].

[8] R. P. Jover, „LTE security, protocol exploits and location tracking experimentation with low-cost software radio," Bloomberg LP, New York, NY, 2016.

[9] T. F. a. W. Wang, „LTE is Vulnerable: Implementing Identity Spoofing and Denial-of-Service Attacks in LTE Networks," Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27606, 2019.

[10] C. A. Hamidreza Ghafghazi, „Security and Privacy in LTE-based Public Safety Network," w *Wireless Public Safety Networks 2*, Elsevier, 2016, pp. 317-364.

[11] L. Guillemot, „Sqimway," [Online]. Available: https://www.sqimway.com/rrc_lte.html. [Data uzyskania dostępu: 27 December 2021].

[12] S. C. Z. C. Chuan Yu, „LTE Phone Number Catcher: A Practical Attack against Mobile Privacy," Wiley, College of Computer, National University of Defense Technology, Changsha, Hunan 410073, China, 2019.

[13] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi i J.-P. Seifert, „Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems," Technische Universität Berlin and Telekom Innovation Laboratories, Aalto University, University of Helsinki, Berlin, Espoo, Helsinki, 2017.

[14] K. Vachhani, „Security Threats Against LTE Networks: A Survey," ECE Department, Nirma University, Ahmedabad, 2018.

[15] J. Jermyn, G. Salles-Loustau i S. Zonouz, „An analysis of DoS attack strategies against the LTE RAN," Journal of Cyber Security, New York, NY, 2014.

[16] M. Kim, J. Park, D. Moon, J. Jang, Y. Kim i J. Lee, „Long-Term Evolution Vulnerability Focusing on System Information Block Messages," University of Science and Technology, Electronics and Telecommunications Research Institute, , Daejeon, Republic of Korea, 2020.

[17] J. Cichonski, J. M. Franklin i M. Bartock, „Guide to LTE Security," NIST (National Institute of Standards and Technology), 2017.

[18] S. X. Zhou, „Investigation of LTE Privacy Attacks by Exploiting the Paging Mechanism," Norwegian University of Science and Technology, Trondheim, 2018.

[19] B. Wojtowicz, „Sourceforge - OpenLTE," [Online]. Available: https://sourceforge.net/p/openlte/wiki/Home/. [Data uzyskania dostępu: 27 December 2021].

[20] Osmocom, „Osmocom Home," [Online]. Available: https://osmocom.org/. [Data uzyskania dostępu: 28 December 2021].

[21] Osmocom, „OsmocomBB Wiki," [Online]. Available: https://osmocom.org/projects/baseband/wiki. [Data uzyskania dostępu: 28 December 2021].

[22] E. Research, „Ettus Research USRP - all products," [Online]. Available: https://www.ettus.com/all-products/usrp-b200mini/. [Data uzyskania dostępu: 28 December 2021].

[23] Osmocom, „RSSI application (firmware)," [Online]. Available: https://osmocom.org/projects/baseband/wiki/Rssibin. [Data uzyskania dostępu: 28 December 2021].

[24] M2Catalyst, LLC., „Google Play store - Network Cell Info Lite," [Online]. Available: https://play.google.com/store/apps/details?id=com.wilysis.cellinfolite. [Data uzyskania dostępu: 28 December 2021].

[25] Simply Advanced, „Google Play store - LTE Discovery (5G NR)," [Online]. Available: https://play.google.com/store/apps/details?id=net.simplyadvanced.ltediscovery. [Data uzyskania dostępu: 28 December 2021].

[26] V. 2. The Single UNIX ® Specification, „sys/socket.h - Internet Protocol family," 1997. [Online]. Available: https://pubs.opengroup.org/onlinepubs/7908799/xns/syssocket.h.html. [Data uzyskania dostępu: 28 December 2021].

[27] 0xh4di, „GSMDecryption - GitHub," 2010. [Online]. Available: https://github.com/0xh4di/GSMDecryption. [Data uzyskania dostępu: 28 December 2021].

[28] A. Kostrzewa, „Development of a man in the middle attack on the GSM Um-Interface," Technische Universität Berlin, Berlin, 2011.

[29] B. Baranoff, „Personal GitHub," 18 grudzień 2021. [Online]. Available: https://github.com/bbaranoff. [Data uzyskania dostępu: 18 grudzień 2021].

[30] ITU-T, „Various tones used in national networks (E.180)," ITU, Geneva, 2003.

[31] P. Panigrahi, 22 June 2017. [Online]. Available: https://www.3glteinfo.com/lte-tracking-area-update-call-flow-procedure/. [Data uzyskania dostępu: 18 December 2021].

[32] Nick, 30 May 2020. [Online]. Available: https://nickvsnetworking.com/srslte-install-for-bladerf-limesdr-on-debian-ubuntu/. [Data uzyskania dostępu: 2021 December 2021].

[33] LimeSDR, 2021. [Online]. Available: https://www.crowdsupply.com/lime-micro/limesdr. [Data uzyskania dostępu: 18 December 2021].

[34] T.-M. PL. [Online]. Available: https://www.t-mobile.pl/c/wylaczamy3g [PL]. [Data uzyskania dostępu: 18 Devember 2021].

[35] WhatNext.pl, 16 November 2020. [Online]. Available: https://www.gov.pl/web/5g/przeczytaj-zbliza-sie-wylaczenie-sieci-3g-dlaczego-nie-2g-i-dlaczego-trzeba-bedzie-wymienic-telefon [PL]. [Data uzyskania dostępu: 18 December 2021].

[36] Telecompaper.com, 26 January 2021. [Online]. Available: https://www.telecompaper.com/news/telenor-norway-announces-3g-switch-off-this-week. [Data uzyskania dostępu: 18 December 2021].