

doi:10.14132/j.cnki.1673-5439.2020.02.006

移动网络用户隐私与信息安全研究

陈发堂,赵昊明,吴晓龙,李阳阳

(重庆邮电大学 重庆邮电大学通信与信息工程学院,重庆 400065)

摘要:移动网络的安全性研究一直是热点问题,目前已知的许多攻击都以知道目标所在位置跟踪区(Tracking Area,TA)为前提,已有的TA定位方法所需条件苛刻且个别方法在5G系统中不再适用。文中提出了一种只需要知道目标手机号,即可实现如TA定位、拒绝服务、强制降级、IMSI获取的攻击方法,并在现网下测试验证了对用户隐私与财产安全造成影响的“GSM嗅探”攻击。由于攻击具有普遍适用性,该工作可以为将来改进和更新相关过程提供基础。

关键词:LTE安全;网络攻击;位置跟踪

中图分类号:TN929.5 **文献标志码:**A **文章编号:**1673-5439(2020)02-0035-06

Privacy and information security of mobile network users

CHEN Fatang, ZHAO Haoming, WU Xiaolong, LI Yangyang

(School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: The research of mobile network security has always been a hot topic. At present, lots of known attacks are based on the premise of knowing the tracking area (TA) at the target location. The existing methods for target locating require rigorous conditions. A few of methods no longer make sense in 5G system. A special method makes a series of attacks only with the phone number. These attacks include TA location, denial of service, forced degradation, and IMSI acquisition. The GSM sniffing attack in the current network is implemented and the impact of the attack on user privacy and property security is verified. Due to the universality of these attacks, the method can provide a foundation for improvements and updates of future study.

Keywords: LTE security; network attack; position tracking

下一代移动通信5G相比于4G网络具有海量连接、低延时、高带宽等特点。初期5G的部署多采用非独立组网的方式,其中可选的一种非独立组网方式为:4G基站、5G基站共用4G的核心网。以上布网方式导致了初期的5G网络仍然容易受到LTE中存在的绝大多数漏洞的攻击^[1]。对蜂窝网络的安全性研究一直是个热点问题^[2-5],这部分的研究将帮助4G网络安全地演进到如今的5G网络,具有重要的现实价值。

用户接入网络后,为了避免国际移动用户识别码(International Mobile Subscriber Identity, IMSI)泄露带来的隐私问题,3GPP标准中规定在附着完成后,核心网应为终端分配唯一的移动用户标识(Temporary Mobile Subscriber Identity, TMSI)来代替IMSI的交互。在LTE系统中使用的是全球唯一临时标识(Globally Unique Temporary Identity, GUTI),GUTI更新频率越快,对用户隐私保护性越好。然而

收稿日期:2020-02-07 本刊网址:<http://nyzr.njupt.edu.cn>

基金项目:教育部—中国移动科研基金(MCM201805-2)资助项目

作者简介:陈发堂,男,研究员,chenft@cqupt.edu.cn

引用本文:陈发堂,赵昊明,吴晓龙,等.移动网络用户隐私与信息安全研究[J].南京邮电大学学报(自然科学版),2020,40(2):35-40.

标准中并没有明确规定 GUTI 如何更新,具体更新方式由运营商决定,若每次重分配后的 GUTI 为随机值,则可以很大程度上提高安全性。通过对三家运营商的测试发现,中国的 GUTI 重分配存在一定安全隐患。

从 2G 到 4G,伪基站(Fake Base Station, FBS)的问题一直存在,其问题本质是网络功能性、成本与安全性之间的矛盾。通过部署高信号强度的 FBS,吸引覆盖区域内的终端向其驻留,将对区域内的终端带来不同程度的影响。其中典型应用为“GSM 嗅探”,但该攻击需要知道目标所在的位置跟踪区(Tracking Area, TA)、目标的手机接入 2G 网络作为前提条件。目前已知的许多攻击,如文献[6]中篡改终端能力信息,文献[3]的中间人攻击与文献[7]域名解析劫持,都需知道目标所处的 TA。

文献[8]提出两种精确定位目标的方法,利用终端收到基站下发的无线资源控制(Radio Resource Control, RRC)重配消息将响应测量报告的特点,因为该消息中携带终端的全球定位系统(Global Positioning System, GPS)位置信息,通过伪造 RRC 重配消息,实现目标定位;利用无线链路切换失败报告,攻击首先在目标相同小区运行一台伪基站,当收到 UE 的位置区域更新(Tracking Area Update, TAU)请求后关闭当前伪基站,同时运行第二台伪基站,终端检测到与之前伪基站失步,启动无线链路失败(Radio Link Failure, RLF)定时器,生成 RLF 报告,并被新伪基站吸引驻留,注册消息中将携带 RLF 报告,该消息中携带终端的 GPS 位置信息,实现目标定位。但这两种攻击都需要知道目标所在的 TA,否则攻击无法实现。文献[9]提出伪造寻呼消息来定位目标的方法,暴力破解目标的 IMSI 后,伪造其 IMSI 寻呼消息,观察是否收到 RRC 连接请求来判定目标是否处在当前小区。该方案虽然能确定目标所处小区,但文中 IMSI 暴力破解所需的时间过长,在此期间目标很可能已经移动,同时 5G 系统已将 IMSI 加密,文中的 IMSI 暴力破解和寻呼将不再适用。文献[2]利用小区无线网络临时标识和 TMSI 相对应的特点实现目标定位。但攻击需要目标终端处在非激活态,且得到目标 TMSI 为前提,在未知目标所处 TA 的情况下不易得到目标 TMSI,且通过发短信的方式触发手机进入连接态容易引起目标警觉。

本文提出了一种只通过目标手机号,即可实现 TA 定位与目标隐私获取的攻击方法。通过该攻击,

攻击者可以在未得知目标的 TA、目标手机未处在 2G 网络的条件下,完成如锁定目标 TA、拒绝服务、强制降级、IMSI 获取的攻击,并在现网下测试了利用攻击完成“GSM 嗅探”的可实施性。由于初期 5G 部署沿用了 LTE 的核心网,且 5G 支持 4G 用户身份识别卡接入 5G 网络,所以本文揭露的漏洞可能在 5G 中依然持续。

1 背景知识

1.1 LTE 网络架构

整个 LTE 网络大致分为以下三个部分:用户设备(User Equipment, UE)、接入网(Evolved UMTS Terrestrial Radio Access Network, E-UTRAN)和演进分组核心网(Evolved Packet Core, EPC)。其中 E-UTRAN 是由多个基站(Evolved Node B, eNodeB)组成,EPC 由移动性管理实体(Mobility Management Entity, MME)、归属用户服务器(Home Subscriber Server, HSS)、服务网关(Serving Gateway, S-GW)以及 PDN 网关(PDN Gateway, P-GW)等网元组成。如图 1 所示为 LTE 网络架构。

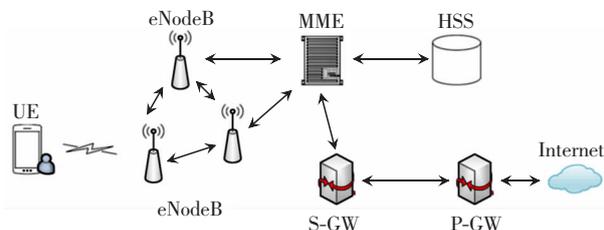


图 1 LTE 网络架构

接下来简要总结各个部分。

UE: UE 是向用户提供服务的移动终端设备,例如手机或平板电脑,通常需要配备运营商提供的通用用户标识模块(Universal Subscriber Identity Module, USIM),该模块中包含永久身份标识(IMSI)。

eNodeB: 即演进型 NodeB, LTE 网络中基站的名称,是 UE 连接到网络的接入点,负责空中接口相关的所有功能。

HSS: 本质上是数据库,用来存储用户的相关信息,例如国际移动用户标识、认证密钥、服务质量简档和漫游限制^[10]。

MME: 移动管理实体,是 EPC 的一个关键控制平面实体,主要的职责是移动性管理、承载管理鉴权认证、S-GW 和 P-GW 的选择等功能。

1.2 4G 系统中的临时身份标识

LTE 系统中将 GUTI 作为用户临时身份标识,

如图 2 所示。GUTI 由两大部分组成:全球唯一的移动性管理实体标识符和 MME 临时移动用户身份。用户临时身份标识由一个临时且唯一的 32 位值组成,该值用于标识 MME 中的 UE。当 UE 连接到网络或更新其跟踪区域时,MME 将 GUTI 分配给 UE。此后,UE 和 MME 使用分配的 GUTI 代替 IMSI 进行 UE 和 MME 之间的标识和通信。



图 2 GUTI 结构

2 目标定位与隐私获取

本节提出了一套完整攻击方法,通过该攻击可实现对目标所在的 TA 跟踪;在确定了 TA 后,可对目标终端进行拒绝服务(Denial of Service, DoS)攻击,强制降级并执行“GSM 嗅探”攻击,获取目标隐私信息。

2.1 TA 区跟踪

寻呼消息中的 TMSI 以明文的形式出现在寻呼信道上,从某种程度上来说,寻呼消息是公开的私有信息。GUTI 分配方式由运营商决定,不安全的分配方式容易导致用户隐私信息泄露。在 LTE 中,只有 GUTI 重分配才能改变设备的 TMSI,协议中规定以下情况将触发 GUTI 重分配:(1) 由网络触发的非接入层 GUTI 重分配过程。(2) 在 TAU 完成后,网络将下发新的 GUTI 标识。(3) 初始附着完成后,网络将下发 GUTI 标识。

若终端不支持或未使用 LTE 语音承载(Voice over LTE, VoLTE)功能,在呼叫时,将会通过电路域回落(Circuit Switched Fallback, CSFB)使用 2G 或 3G 来支持电路交换的语音通话,通话过程如图 3 所示。当 UE 收到广播的寻呼消息,将会回应扩展服务请求消息,此后将断开与 LTE 网络的连接,进行 2G/3G 下的语音通话。语音通话结束后将发起 TAU 过程重新返回 LTE 网络,该过程会重新分配 GUTI,从而实现了每次拨打电话后用户临时身份标识的更新。

终端若开启了 VoLTE 功能,在拨打电话时不会脱离 LTE 网络,所以不会触发 TAU 过程使得 GUTI 重分配。重分配主要由周期性 TAU 来完成,但现网测试表明,中国运营商设置的 TAU 周期过长,其中最短约 1 小时,而最长为 2 小时。在此时间间隔内攻击者可以通过静默呼叫的方式,触发网络对目标 UE 的寻呼,若和目标的位置区域相同,将会在寻呼

消息中监听到重复的 TMSI。

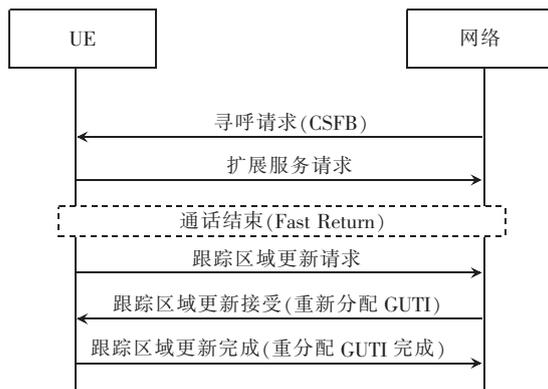


图 3 由 CSFB 导致的 GUTI 重分配

为了完成对未开启 VoLTE 的目标定位。实验首先部署了一套低成本、实时的 LTE 寻呼信道监听装置,硬件使用 USRP B210^[11],这是一款通过软件来控制收发操作的无线电装置;软件使用开源软件 srsLTE^[12]修改了程序 pdsch_ue 的代码,实现了对下行共享信道寻呼消息的实时监听。图 4 为所监听小区的部分寻呼消息的 ASN.1 编码。针对三家运营商我们分别进行了 200 次 CSFB 呼叫,测试发现 GUTI 重分配后的 TMSI 值变化规律相同,都未满足随机性的要求。

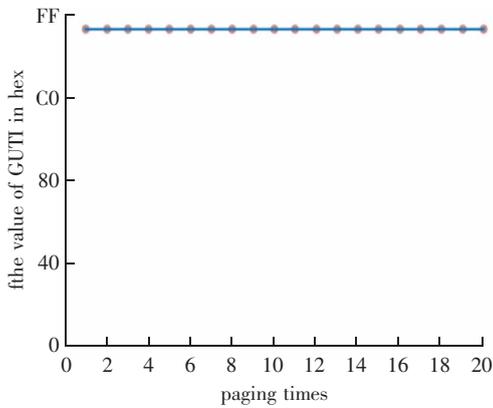
```
Setting sampling rate 23.04 MHz
- PCI: 325 5.7, FrameCnt: 0, Sta
- Nof ports: 2
- CP: Normal
- PRB: 100
- PHICH Length: Normal
- PHICH Resources: 1
- SFN: 180
Decoded MIB. SFN: 180, offset: 0
[40 00 4d 11 d3 61 b0 ];
[40 00 2d d2 01 94 80 ];
[40 80 4f d3 c7 35 40 01 ce 0d d2 47 00 ];
[40 00 2d 9f 0b c7 b0 ];
[40 00 3c 14 4b c2 20 ];
[40 00 1e 7b 4b b3 20 ];
```

图 4 监听的部分寻呼消息

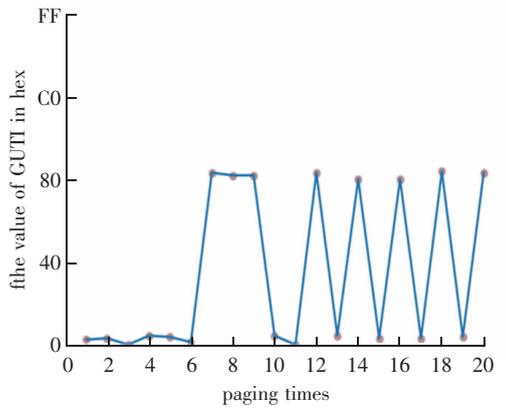
GUTI 中 TMSI 有 4 个字节,其中第一个字节仅在移动管理实体编号(Mobility Management Entity Code, MMEC)改变时发生变化,而相同的 MMEC 会持续 30 次左右,在此期间内第一个字节值始终不变。MMEC 变化将引起第一个字节改变,但变化后的规律和之前相同,在接下来一定次数的呼叫内,第一个字节始终不会发生改变;第二个字节前 4 比特为固定值,具体的固定值和 MMEC 有关,如图 5 所示,前 4 比特被固定为 0000 和 1000;剩余 20 个比特为随机值。32 比特的临时身份中 12 个比特有规律地出现,这增加了用户隐私信息被泄露的风险。即使 CSFB 呼叫引起终端 TMSI 改变,攻击者依然可以通过已经发现的规律实施对目标的用户位置跟踪区定位。值得注意的是,其中一家运营商在正常呼叫

和静默呼叫时 GUTI 重分配呈现了不同的规律。正常呼叫时的变化规律和前文相同,但静默呼叫时如

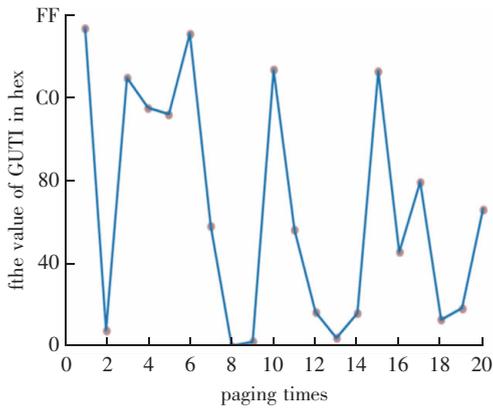
图 6 所示,TMSI 有 3 个字节不会改变,唯一改变的字节也是呈规律性变化。



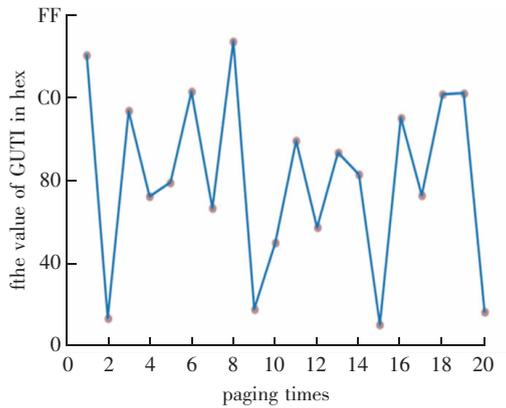
(a) TMSI 中第一字节



(b) TMSI 中第二字节



(c) TMSI 中第三字节



(d) TMSI 中第四字节

图 5 GUTI 中 TMSI 变化规律

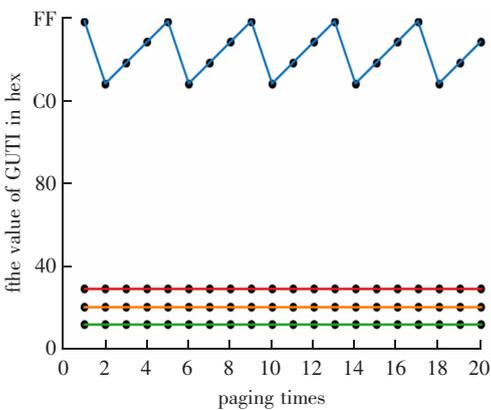


图 6 某运营商在静默呼叫的重分配情况

对于开启 VoLTE 的终端,实验统计了 72 小时由周期性 TAU 导致的 GUTI 重分配情况。在 72 小时内共触发 75 次周期性 TAU,即 UE 在约 1 小时左右会发起一次 TAU 从而触发 GUTI 重分配。由于周期性 TAU 并不会引起 MMEC 改变,所以在 72 小时中 TMSI 变化规律一直未变。

图 7 提出了 TA 区跟踪攻击模型,攻击者只需知道目标的手机号即可完成定位。

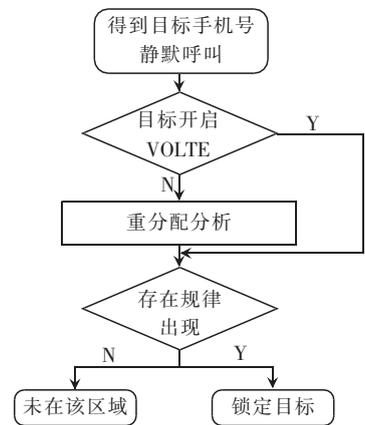


图 7 TA 定位攻击流程

2.2 强制终端降级与 DoS 攻击

根据 3GPP 标准^[13]中描述:当终端的连接请求被网络拒绝后,网络下发的拒绝消息中会携带演进的移动管理原因值(Evolved Mobility Management

Cause, EMM Cause) 来告知被拒绝的原因。基于网络给终端下发的拒绝消息未受完整性保护和加密的特点,攻击者通过前置攻击锁定目标所在区域后,伪造拒绝原因值来操作终端,如图 8 所示。这种攻击部署简单但影响极大。

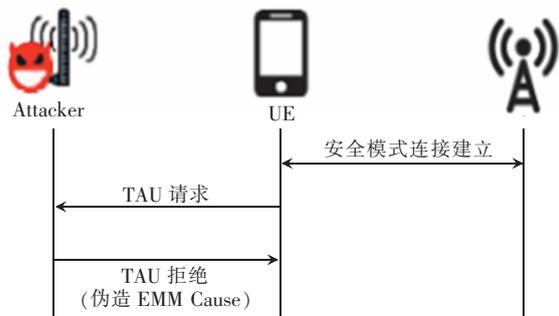


图 8 利用 EMM Cause 的 FBS 攻击

表 1 汇总了经现网测试后,攻击者可能利用的部分原因值与造成的影响。

表 1 拒绝原因及影响

原因值 ID	拒绝原因	影响
3	非法 UE	DoS 攻击
6	非法 ME	DoS 攻击
7	禁止 EPS 服务	强制降级
8	禁止 EPS 与非 EPS 服务	DoS 攻击
9	UE 身份网络无法识别	IMSI 隐私泄露
15	区域内没有合适的小区	IMSI 隐私泄露

2.3 现网测试情况

由前文所述,若目标手机开启了 VoLTE 功能会导致终端 TMSI 仅在 TAU 时改变,且国内运营商设置的 TAU 周期为一小时以上,所以定位用户极其容易,实验主要测试目标关闭 VoLTE 的情况。通过 CSFB 采取静默呼叫的方式监听拨出后 2~5 秒的寻呼消息。在电话拨出 2~4 秒后挂断电话。采用静默呼叫时,目标 UE 不会响铃但会触发网络对目标的寻呼,通过这种方式将使目标无法察觉。当与目标处于同一位置跟踪区时,拨打 7 次后发现,存在部分 TMSI 的第一个字节始终为 F4,且第二个字节都以十六进制数字 0 和 8 为开头;随后又拨打了 3 次电话,出现了相同规律变化的 TMSI,可以确定主叫和目标处在相同的位置区域。

锁定目标所在区域后,通过目标手机号前 3 位得知目标为移动用户,将手机插入相应运营商 SIM 卡,通过工程模式获取到当前区域的 TAC 为 13149, MCC 和 MNC 信息为 460/00,当前终端工作在

2 624.6 MHz;将伪基站的 TAC 设置为 1,保证了该 TAC 未在 TA 列表内,工作频率和 MCC/MNC 设置为相同值,吸引终端发起 TAU 过程。伪基站硬件部分包括两台 Linux 操作系统的主机和射频模块 USRP B210;软件部分使用开源软件 OAI^[14],两台主机分别部署 OAI 的核心网部分和基站部分。实验以原因值 7 拒绝,测试发现目标降为 2G。随后实验手机输入目标手机号登录其支付宝账号,并部署“GSM 嗅探”装置,顺利嗅探到验证短信如图 9 所示,至此完成攻击。

```

▶ Frame 189: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▶ Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▶ User Datagram Protocol, Src Port: 58842, Dst Port: 4729
▶ GSM TAP Header, ARFCN: 0 (Downlink), TS: 1, Channel: SDCCH/8 (0)
▶ Link Access Procedure, Channel De (LAPDm)
▶ GSM A-I/F DTAP - CP-DATA
▶ GSM A-I/F RP - RP-DATA (Network to MS)
▼ GSM SMS TDM (GSM 93.40) SMS-DELIVER
0..... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
0..... = TP-UDHI: The TP UD field contains only the short message
...i.... = TP-SRT: A status report shall be returned to the SME
....0... = TP-LP: The message has not been forwarded and is not a spawned message
....i... = TP-MMS: No more messages are waiting for the MS in this SC
...-00 = TP-MTI: SMS-DELIVER (0)
▶ TP-Originating-Address - (95188)
▶ TP-DCS: 0
▶ TP-PID: 0
▶ TP-Service-Centre-Time-Stamp
▶ TP-User-Data-Length: (100) depends on Data-Coding-Scheme
▼ TP-User-Data
SMS text: 登录验证码: 3468. 支付宝全力保护您的账户安全,验证码请勿泄露给他人。唯一热线95188【支付宝】
0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....E
0010 00 43 4e 78 40 09 40 11 ee 2f 7f 09 09 01 7f 09 CNU@ / .....
0020 00 01 05 da 12 79 00 2f fe 42 02 04 01 01 00 00 ...y / B .....
0030 e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....G -- 1.80
0040 10 65 2f 4e d8 5b 9d 30 11 2b 2b 2b 2b 2b 2b e/N | 0 +++++
0050 2b

```

图 9 下行短信监听

3 结束语

本文研究了现网中的设计缺陷,并利用这些缺陷提出了从定位用户到强制目标降级、DoS 攻击、IMSI 信息获取的一套完整攻击。分析了这些攻击在 5G 系统下的可实施性。经现网测试表明,在 LTE 和 5G 网络初期,攻击者利用这些漏洞可以顺利完成攻击。这种攻击具有普遍适用性,因此这项研究非常重要,并且该研究可以为将来改进和更新相关过程提供基础。

参考文献:

- [1] JOVER R P, MAROJEVIC V. Security and protocol exploit analysis of the 5G specifications [J]. IEEE Access, 2019, 7: 24956 - 24963.
- [2] RUPPRECHT D, KOHLS K, HOLZ T, et al. Breaking LTE on layer two [C] // IEEE Symposium on Security & Privacy. 2019.
- [3] BASIN D, DREIER J, HIRSCHI L, et al. A formal analysis of 5G authentication [C] // ACM SIGSAC Conference on Computer and Communications Security. 2018.
- [4] KOUTSOS A. The 5G-AKA authentication protocol privacy [C] // IEEE European Symposium on Security and Privacy. 2019.
- [5] HONG B, BAE S, KIM Y. GUTI reallocation demystified: cellular location tracking with changing temporary identifier

- [C] // Network and Distributed System Security Symposium. 2018.
- [6] SHAIK A, BORGAONKAR R, Park S, et al. New vulnerabilities in 4G and 5G cellular access network protocols; exposing device capabilities [C] // Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks. 2019.
- [7] HUSSAIN S R, CHOWDHURY O, MEHNAZ S, et al. LTE inspector: a systematic approach for adversarial testing of 4G LTE [C] // Network and Distributed System Security Symposium. 2018.
- [8] SHAIK A, BORGAONKAR R, ASOKAN N, et al. Practical attacks against privacy and availability in 4G/LTE mobile communication systems [C] // Network and Distributed System Security Symposium. 2015.
- [9] HUSSAIN S R, ECHEVERRIA M, CHOWDHURY O, et al. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information [C] // Network and Distributed System Security Symposium. 2019.
- [10] FIRMIN F. The Evolved Packet Core [EB/OL]. [2019-12-09]. <http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core>.
- [11] Ettus Research. USRP B210 [EB/OL]. [2019-12-09]. <https://www.ettus.com/all-products/UB210-KIT>.
- [12] Andrepuschmann. srsLTE [EB/OL]. [2019-12-09]. <https://github.com/srsLTE/srsLTE>.
- [13] 3GPP. Non-Access-Stratum protocol for Evolved Packet System; TS 24.301 [S]. 2017.
- [14] OpenAir Interface Software Alliance. OpenAirInterface [EB/OL]. [2019-12-09]. <https://www.openairinterface.org/>.